APX-110N5
&
APX-120N5

Outdoor IP67 IEEE 802.11a/n Wireless

AP/Client/Bridge, And Preconfigured Wireless Bridge

w/Built-in 19dBi@5GHz Antenna

User Manual

Version 1.1

www.antaira.com

LEGAL

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. Our company assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. Our company reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

Our company makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor do we assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

Our products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use our product for any such unintended or unauthorized application, the Buyer shall indemnify and hold Our company and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that we were negligent regarding the design or manufacture of said product.

TRADEMARKS

Microsoft is a registered trademark of Microsoft Corp.
HyperTerminal™ is a registered trademark of Hilgraeve Inc.

WARNING:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference in which case the user will be required to correct the interference at their own expense. NOTICE: (1) The changes or modifications not expressively approved by the party responsible for compliance could void the user's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

WARNING:

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Outdoor Wireless Bridge

IP67 IEEE802.11a/n Wireless Bridge, w/built-in 19dBi@5GHz Antenna

User Manual
Version 1.0 - April 15, 2014

This manual supports the following models:
APX-110N5
APX-120N5

This document is the current official release manual. Please check our website (WWW.Antaira.com) for any updated manual or contact us by E-mail (info@antaira.com).

©2013-2014

All Rights Reserved

The contents of this document are subject to change without any prior notice.

Table of Contents

Overview **6**
Introduction **6**
Features 6
Benefits 7
Package Contents 8
Hardware Description **9**
Physical Dimension 9
Front Panel 10
Side View 10
Back View 11
LED Indicators 11
Hardware Installation **12**
Installation Steps 12
Mounting Installation **13**
Pole Mounting 13
Antennas and Cables **14**
Antenna 14
Ports 14
10BaseT/100BaseTX Pin Assignments 14
Cabling 15
Operation Modes & Connection Examples **16**
APX-120N5 Pre-Configured Bridge **16**
Preconfigured Bridge Access Point 17
Preconfigured Bridge Station 18
Access Point and Access Point WDS Mode **19**
Station Mode 19
Station WDS Mode 20
Repeater WDS Mode 20
Configure the Computers IP Address **21**
For Windows 95/98/98SE/ME/NT 21
For Windows XP/2000 22
Logging onto the APX-110N5/APX-120N5 ..... **23**
Navigation **25**
Main Menu Bar 25
Changing the units IP Address 25
How to save changes 26
Basic Network Tab **27**
Network Mode: Bridging 27
LAN Setup 27
Basic Wireless Tab **30**

Basic Wireless Settings....30
Wireless Mode....30
Access Point Parameters Settings....31
Station Parameters Settings....34
Wireless Security....36
Advance Wireless Tab....41
Long Range Parameters Setup....41
Services Tab....43
Ping Watchdog....44
Auto-Reboot....44
SNMP Setup....45
NTP Setup....45
Web HTTP Security....45
Telnet Access Setup....46
SSH Access Setup....46
System Log Setup....46
System Tab....47
Firmware Upgrade....47
Host Name....48
Administrative and Read-only Account....48
Configuration Management....49
Device Maintenance....49
Status Page....50
Status Reporting....50
Clients Connection Status in AP Status Info....52
Station Connection Info....53
More Status....54
VLAN Tab....56
VLAN Switch....56
VLAN Management....57
Appendix I - Network....58
Appendix III- Advanced Settings....60
Appendix IV- Services....63
Appendix V- VLAN Setup examples....65
A) Tagged Wireless VLAN to Tagged Ethernet VLAN Setup....65
B) Untagged Wireless VLAN to Tagged Ethernet VLAN setup....66
C) Tagged VLAN Pass-Through....66
Technical Specification....67

Overview

Introduction

Antaira's APX-110N5 & APX-120N5 high performance Wireless Bridge is a managed device that supports IEEE-802.3a/n wireless communication standards. The wireless device supports long range high speed communication of up to 300Mbps.
These models are suitable for more applications, capable of being powered from either the 24 or 48 volt PoE standard. The built in antenna is a 5GHz 19dBi Dual-polarization antenna, the unit supports an operating temperature of -20°C ~ 70°C.
Units come with the following security features; Hidden SSID, MAC address filtering, WEP (Wired Equivalent Privacy) in 64 and 128 bit as well as IEEE 802.11i and 802.1x security authentication.

Features

- System Interface/Performance
  - Point-to-Point Wireless Bridge
  - Internal Antenna Signal Strength Indication by Web console
  - IEEE 802.11a/n Compliant
  - IEEE 802.11i / i02.1x Authentication
  - Maximum data Rate: 300Mbps
  - Supports QoS
- Power Supply
  - PoE / PD (Power Device) IEEE 802.3af compliant
- Operating Temperature
  - Standard Operating Temperature model: -20°C ~ 70°C
- Case/Installation
  - IP67 Outdoor Waterproof Housing Design
  - Built-in 5GHz 19dBi Dual-polarization antenna
  - Adjustable Antenna Elevation (25 º Up/Down)
  - Pole Mount Design
- Grounding Terminal located within the mounting
- 2 Year Warranty

Benefits

APX-120N5

The APX-120N5 provides the user with two wireless units already set up in a preconfigured pair. These units have custom firmware loaded providing the units with IP addresses, ESSID, Security Encryption and the best wireless operation settings for standard deployment. This allows the APX-120N5 to be used in plug and play rapid deployment applications where software changes are not required.

Point-to-Point

Point-to-Point communication between different locations allows the user too bridge wireless clients that are kilometers apart.

Highly Secured Wireless Network

The units are IEEE802.11i compliant and supports IEEE 802.1x for secure authentication. The wireless bridge supports EAP-TTLS and EAP-PEAP.

HTTPS

The access point supports HTTPS (SSL) in addition to the standard HTTP. HTTPS (SSL) features additional authentication and encryption for secure communication.

Telnet

Telnet allows a computer to remotely connect to the access point CLI (Command Line Interface) for control and monitoring.

SSH

SSH (Secure Shell Host) establishes a secure host connection to the access point CLI for control and monitoring

Package Contents

APX-120N5– Outdoor IP67 IEEE 802.11a/n Wireless Bridge with Built in 19dBi@5GHz Antenna

- APX-120N5-1 (AP WDS)
- APX-120N5-2 (Station EDS)
- User Manual CD (Security Key sticker on CD)
- Quick Installation Guide
- Pole-mount Kit
- Rubber grommet for waterproof RJ45

APX-110N5– Outdoor IP67 IEEE 802.11a/n Wireless Bridge with Built in 19dBi@5GHz Antenna

- User Manual CD
- Quick Installation Guide
- Pole-mount Kit
- Rubber grommet for waterproof RJ45

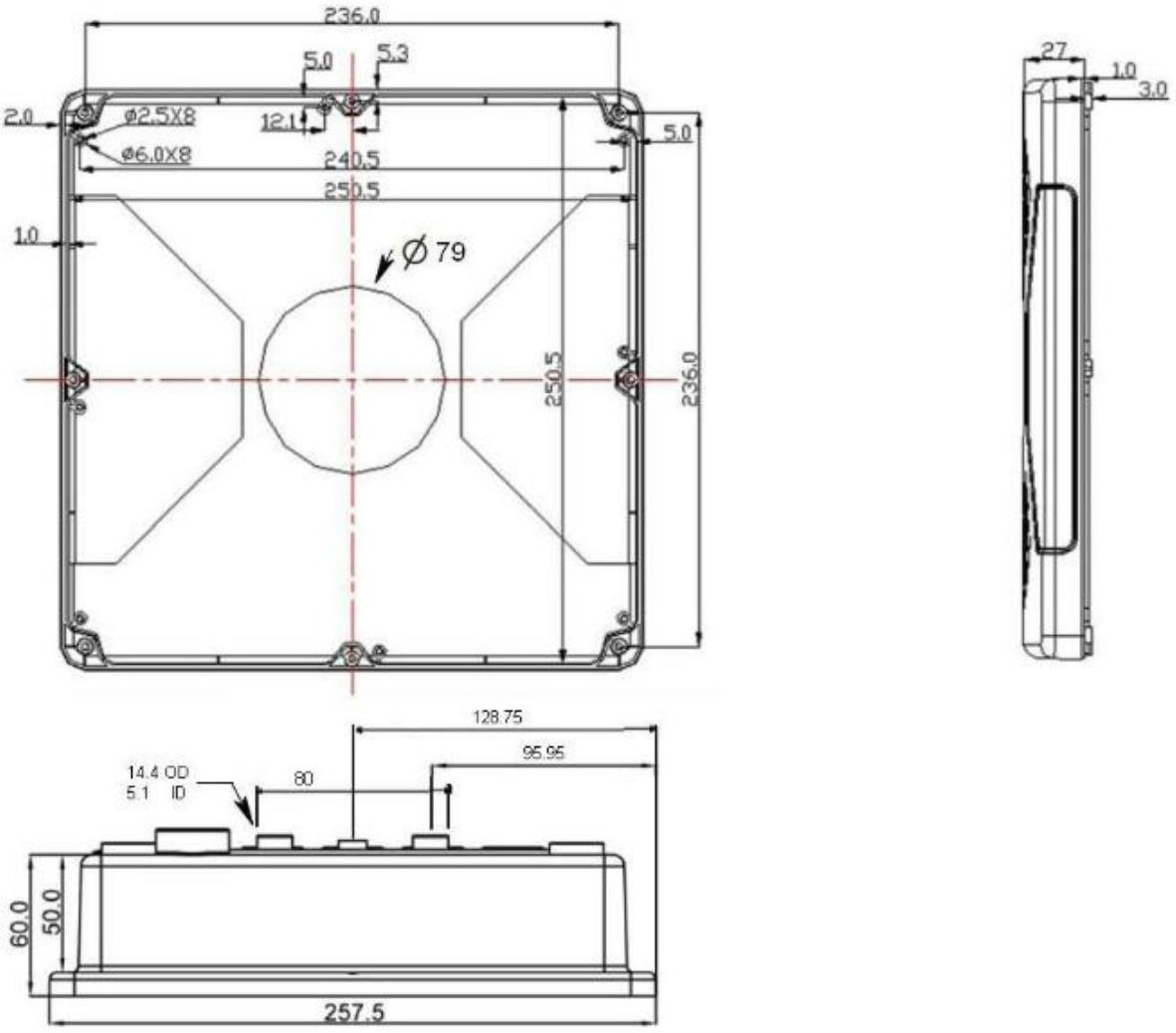
Compare the contents of the wireless device with the checklist above. If any item is damaged or missing, please contact Antaira or Antaira's authorized channel partners for service.

Hardware Description

The Wireless devices hardware spec, port, cabling information, and wiring installation will be described.

Physical Dimension

APX-110N5 & APX-120N5
Dimension: (W x D x H) is 257mm x 86mm x 257mm



Front Panel

The Front Panel of the Wireless Device is shown below:

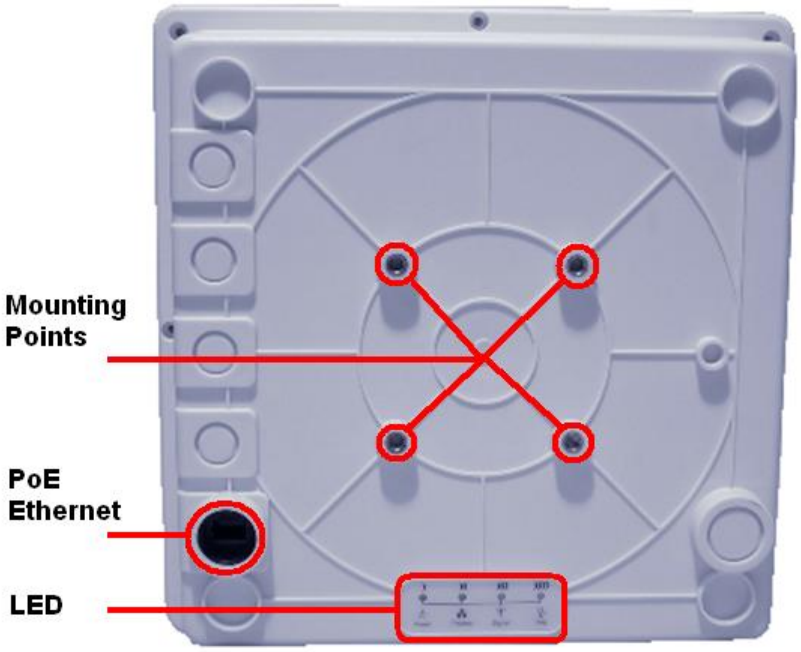
Front Panel of the Wireless Device

Side View

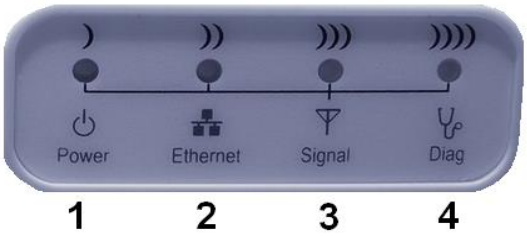
Side View of the Wireless Bridge

Back View

The back panel of the APX-110N5/120N5 includes the PoE Ethernet connection, mounting points and LED diagnostic.



LED Indicators



The diagnostic LEDs located on the front panel of the industrial switch provide real-time information of the system and optional status. The following table provides the description of the LED status.

LED	Color	Description	
1	Red	On	Power is being received
		Off	No power is received by the device
2	Green	On	A link to a switch or PC is present
		Off	No connection has been established
3	Green	On	Sufficient signal strength to establish a connection
		Off	No wireless connection has been made
4	Green	On	When a connection has been made
		Off	When device is first powered on or no connection

Hardware Installation

This section is to explain how to install the APX-110N5 or APX-120N5 Outdoor IP67 wireless bridge.

Installation Steps

Note: It is suggested to log onto the unit in a test environment and change the IP addresses of the units to match the subnet of the network before connecting the devices directly to the main network.

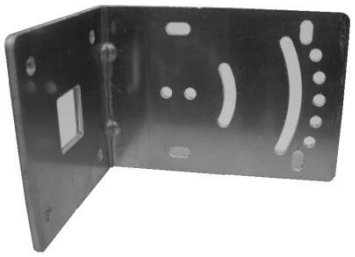
1. Unpack the unit from the box
2. To mount the outdoor wireless bridge, please refer to the **Mounting Installation** section.
3. Power on the unit by connecting an IEEE 802.3af PoE RJ45 cable to the RJ45 port on the back of the unit. The power LED on the wireless bridge will turn on. Please refer to the **LED Indicators** section for indication of LED lights.
4. Once an Ethernet connection has be made it is then possible to log onto the device.

Mounting Installation

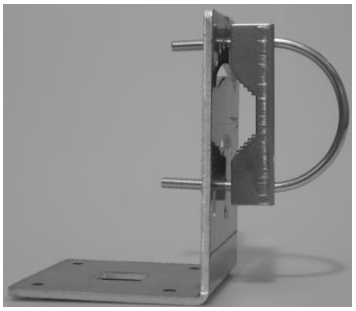
Pole Mounting

Select an elevated location free of large buildings, metal structures and trees within the line of sight between the two bridging units. These obstructions will reduce the distance and throughput capabilities of the units.

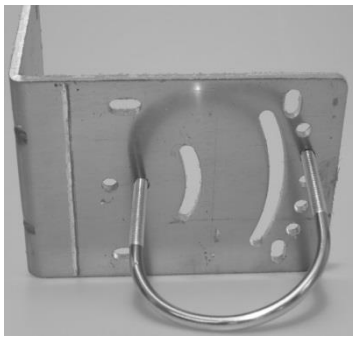
1. Align and attach the metal “L” shaped bracket to the back of the unit with the screws and washers provided.



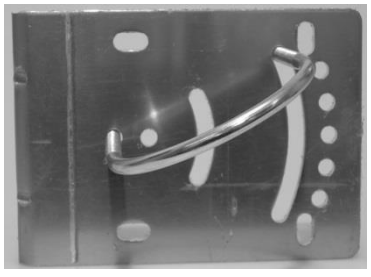
2. Use the metal “U” shaped pole grip to fasten the metal “L” shaped mounting plate to a pole.



   a. Fixed mounting intervals can be used, which provide 5 degrees of change per hole



   b. The sliding mounting option can also be used and might provide more precise tuning for a better connection and throughput.



Antennas and Cables

Antenna

The units have an integrated 5GHz Antenna that is 19dBi

Ports

- **RJ-45 ports**

The (RJ-45) Fast Ethernet ports will auto-sense for 10Base-T or 100Base-TX connections. Auto MDI/MDIX means that the switch can connect to another switch or workstation without changing straight through or crossover cabling. Please refer to the table below for RJ-45 pin assignment.

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45

Cable Types and Specifications

10BaseT/100BaseTX Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

- **RJ-45 Pin Assignments**

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

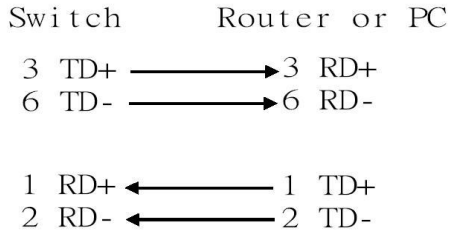
Note *"+" and "-" signs represent the polarity of the wires that make up each wire pair.*

The port on this wireless device supports automatic MDI/MDI-X operation; The user can use straight-through cables (See figure below) for all network connections to injectors, switches or PC. With straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3 and 6 at the other end of the cable. The table below shows the 10BASE-T/100BASE-TX MDI and MDI-X port pin outs.

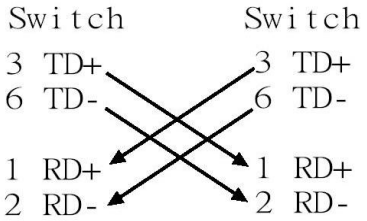
Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

MDI/MDI-X

The following figures show the cable schematic for both straight-through type and crossover type.



Straight Through Cable Schematic



Cross Over Cable Schematic

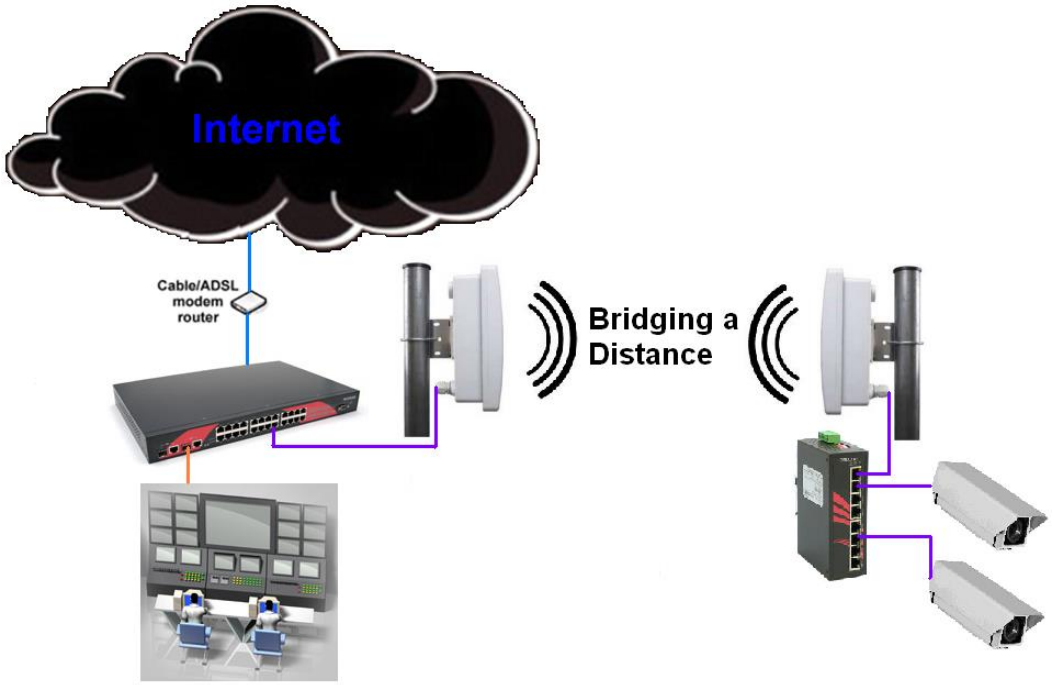
Cabling

- Twisted-pair segments can be connected with an unshielded twisted pair (UTP) or shielded twisted pair (STP) cable. The cable must comply with the IEEE 802.3u 100Base TX standard (e.g. Category 5, 5e, or 6). The cable between the equipment and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.

Operation Modes & Connection Examples

APX-120N5 Pre-Configured Bridge

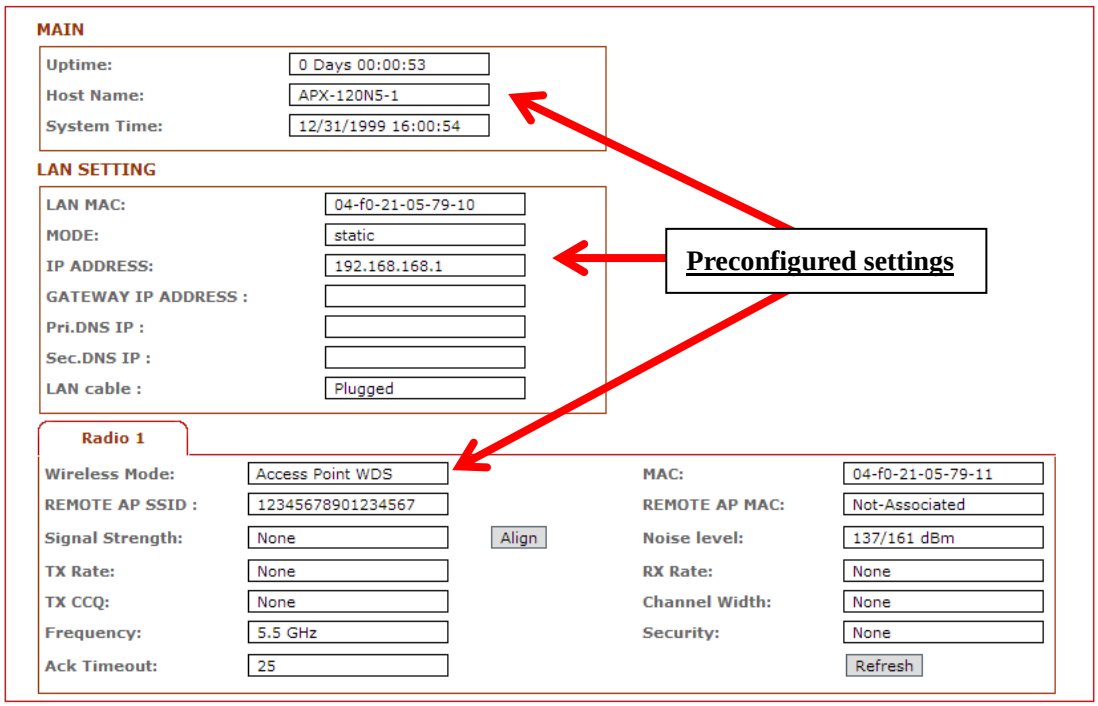
The APX-120N5 will be sold in a pair of units that have been previously configured to connect to one another upon being powered on. The user should change the units IP addresses to match their subnet to prevent any networking conflicts. Once the units have been installed, and a connection between the two units has been established it is then possible to transmit traffic to and from the network.



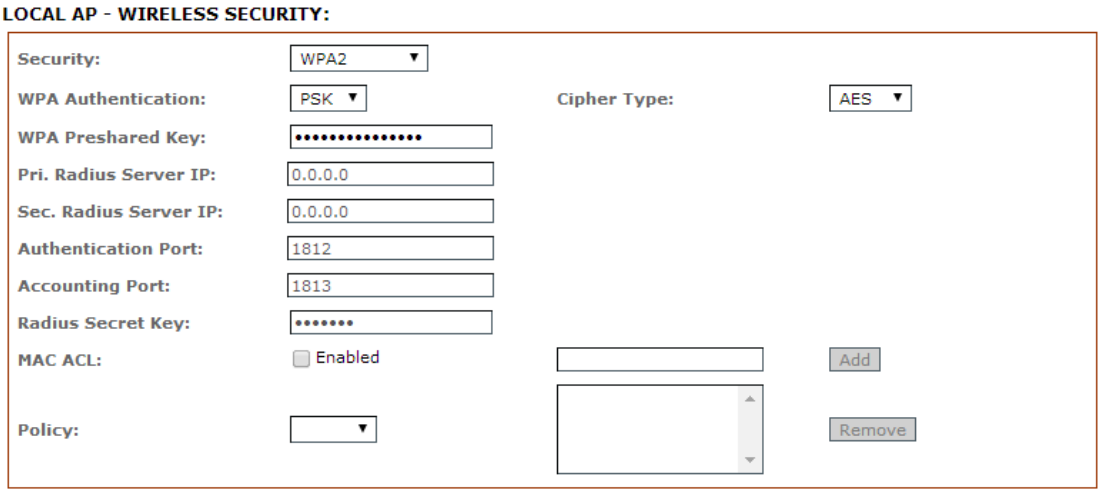
The preconfigured bridge is ideal for quickly deploying and establishing a connection between the main network and a more remote location at the facility. The preconfigured pair of unit will have one unit set up as an Access Point WDS and the second unit will be configured as a Client WDS unit.

Preconfigured Bridge Access Point

The Access Point WDS device APX-120N5-1 will have the following landing page. As shown below the unit is already equipped with an ESSID name, IP address and the wireless mode

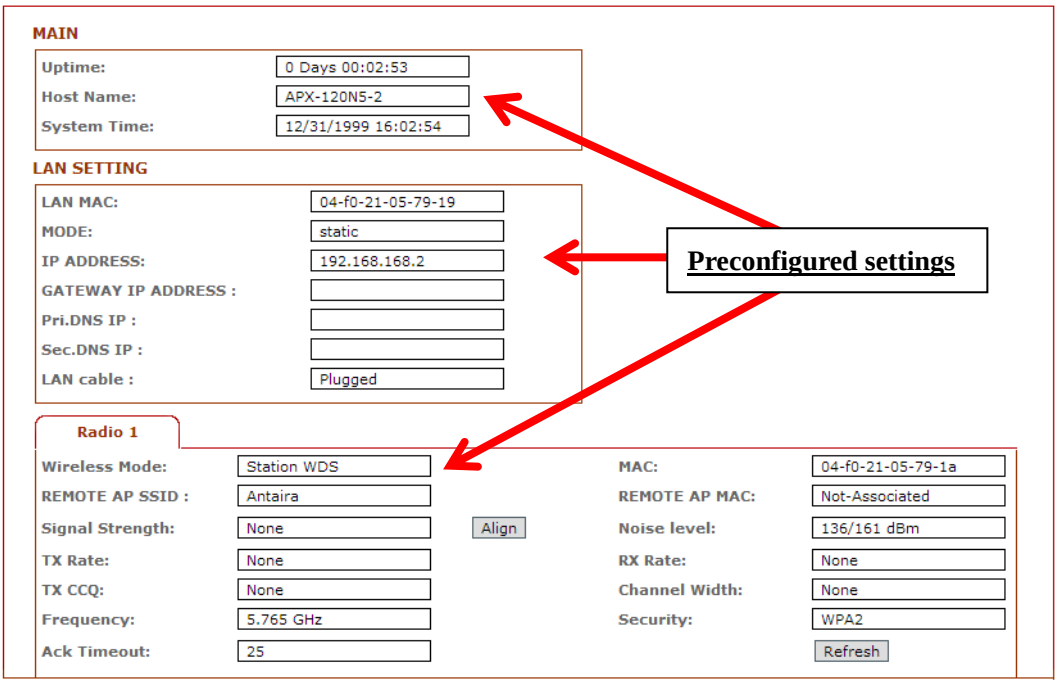


The Access Point WDS unit will also be equipped with preconfigured security encryption features as shown below.

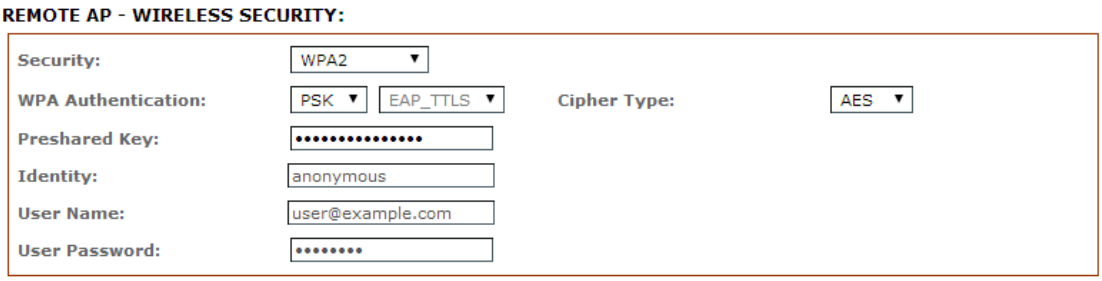


Preconfigured Bridge Station

The Station WDS device APX-120N5-2 will have the following landing page. As shown below the unit is already equipped with the information required to automatically connect to the associated Access Point.



The Station WDS unit will similarly be equipped with preconfigured security encryption that will automatically connect to the associated access point. The user will not have to enter a security key to establish an initial communication connection.



**Notes:

- The security Key for the units will be unique and can be located on the product CD within the original box.
- If a situation arises where the user needs to reset the units, there is an option to reset the devices to the factory default settings within the web console.
    - When using the factory default reset, the units will reestablish a link to one another. Although, the security settings on the units will change to a randomized code that the end user can change by logging into the unit.

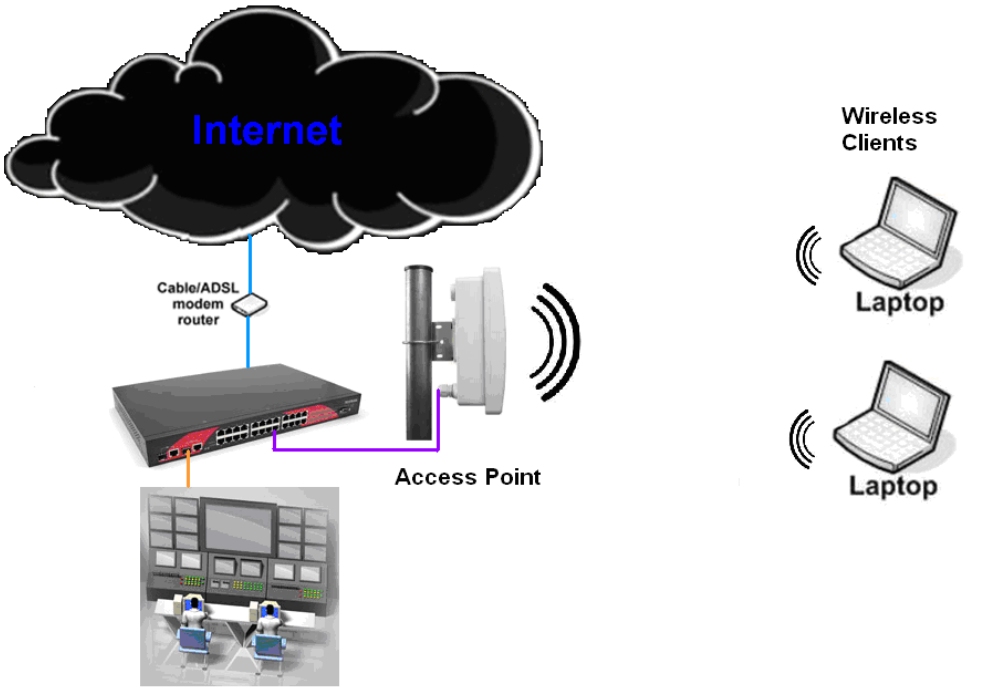
**Other Features

Higher security features and other advanced settings can be customized in the APX-120N5 but is only suggested for more advanced users that are more familiar with wireless communication features.

Below are the standard features for APX-110N5 and for advanced users of the APX-120N5.

Access Point and Access Point WDS Mode

The Access Point operation Mode of the device enables the bridging of wireless clients to wired network infrastructure. Once a connection has been enables, transparent access and communication with each client device to the main network is then possible.
The illustration below shows a typical resources sharing application example using this device. The wireless users are able to access the file server connected to the switch, through the access point in Access Point Mode.



Station Mode

In Station mode the device acts as a wireless client.
When connected to an access point, it creates a network link between the Ethernet network connected at this client device, and the wireless Ethernet network connected at the access point.

In this example the workgroup PCs on the Ethernet network connected to the Station device can access the printer across the wireless connection to the access point where the printer is connected.

Station WDS Mode

Station WDS mode is similar to Station mode. The difference is Station WDS must connect to access point configured to Access Point WDS (or RootAP) mode. Station WDS is mainly use for point-to–point connection between 2 buildings or locations as far as several kilometer away.

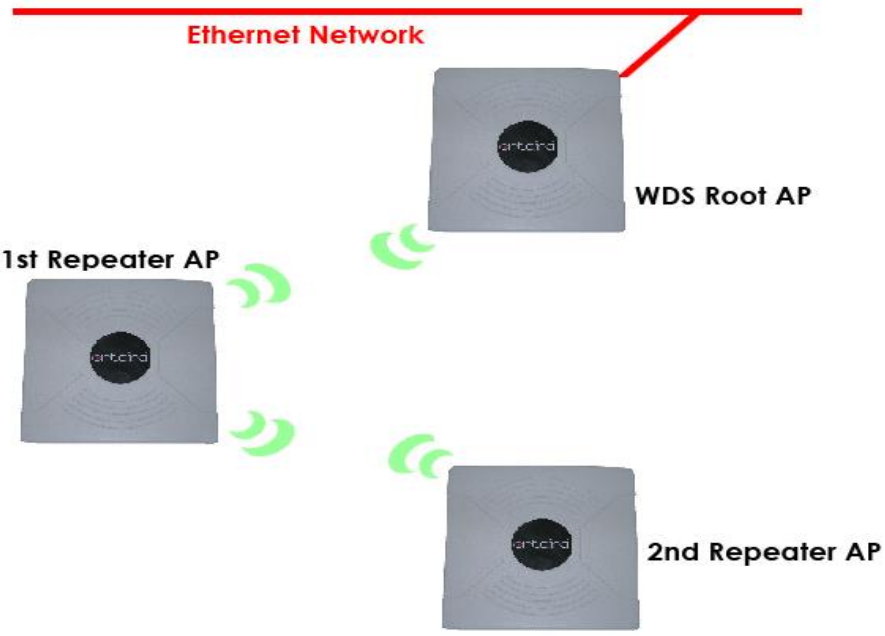
Repeater WDS Mode

Repeater WDS Mode to mainly to extend the wireless range and coverage of the wireless network allowing access and communications over places generally difficult for wireless clients to connect to the network.

In Repeater mode, the access point acts as a relay for network signals on the network by regenerating the signals it receives, and retransmitting them to main network infrastructure.

Detailed information on the Repeater mode is available in the Repeater Setup section.

**** Note: Repeater WDS requires the access point to be setup in RootAP or Access Point WDS mode to work.**



Configure the Computers IP Address

After setting up the hardware you need to assign an IP address to your PC so that it is in the same subnet as the access point.

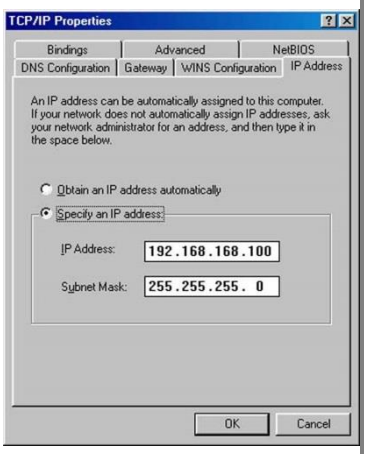
For Windows 95/98/98SE/ME/NT

Step 1:

From your desktop, right-click the **Network Neighborhood** icon and select **Properties**.

Step 2:

Select the network adapter that you are using, then right-click and select **Properties**.



Step 3:

Highlight **TCP/IP** and click on the **Properties** button.

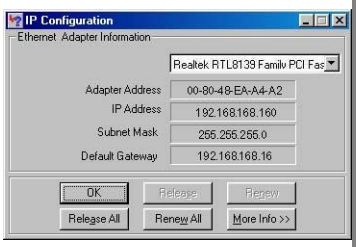
Step 4:

Select the **Specify an IP address** radio button.

Set the IP address to 192.168.168.X and subnet mask to 255.255.255.0, where X can be any number from 2 to 254.

Step 5:

To verify that the IP address has been correctly assigned to your PC, go to the **Start** menu, select **Run**, and enter the command: *winipcfg*.



Select the Ethernet adapter from the drop-down list and click **OK**.

PC is now setup with a proper IP address to communicate with the access point.

For Windows XP/2000

Step 1:

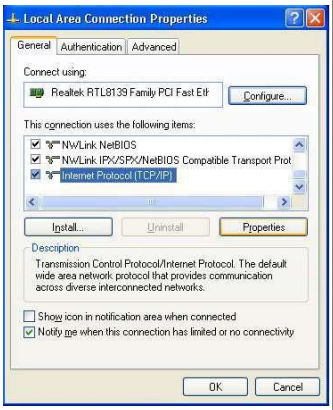
Go to your desktop, right-click on the **My Network Places** icon and select **Properties**.

Step 2:

Right-click the network adapter icon and select **Properties.**

Step 3:

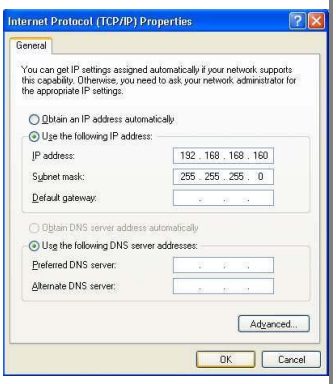
Highlight **Internet Protocol (TCP/IP)** and click on the **Properties** button.



Step 4:

Select the **Use the following IP address** radio button.

Set the IP address to 192.168.168.X and subnet mask to 255.255.255.0, where X can be any number from 2 to 254.

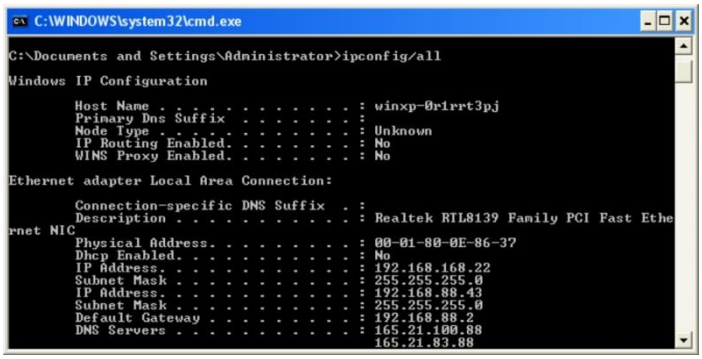


Step 5:

Click on the **OK** button to close all windows.

Step 6:

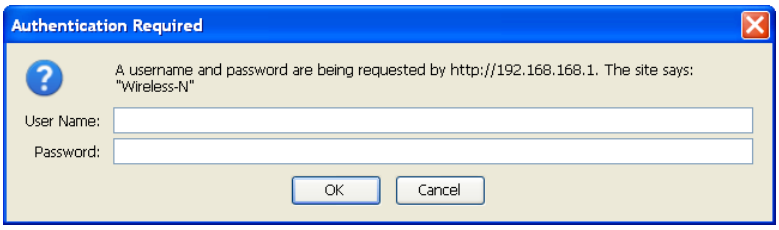
To verify that the IP address has been correctly assigned to the PC, go to the **Start** menu, **Accessories**, select **Command Prompt**, and type the command: *ipconfig/all*



PC is now setup with a proper IP address to communicate with the access point.

Logging onto the APX-110N5/APX-120N5

By opening an internet browser and typing in the default IP address 192.168.168.1 the user will be prompted with a login screen.

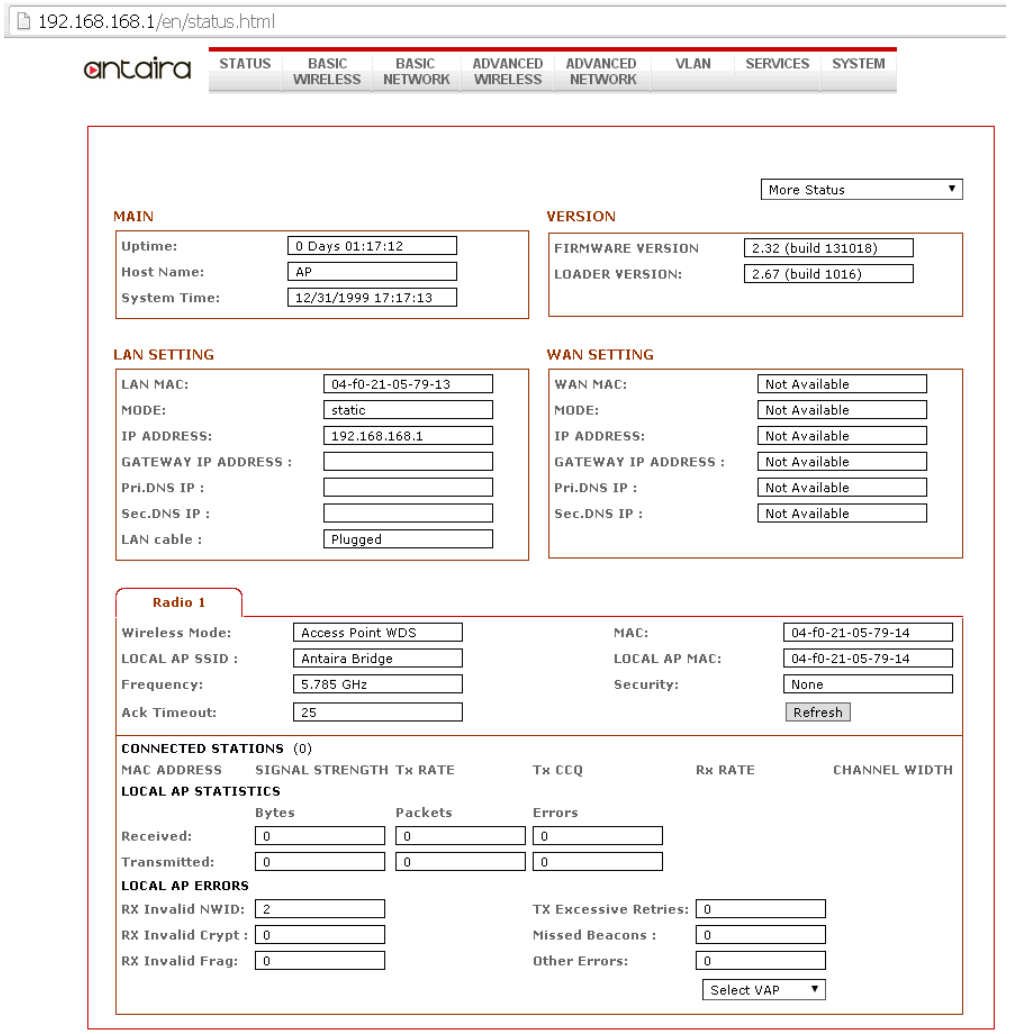


The default settings are

Username: admin

Password: password

The user will then be redirected to the web console page.


192.168.168.1/en/status.html
antaira
STATUS
BASIC WIRELESS
BASIC NETWORK
ADVANCED WIRELESS
ADVANCED NETWORK
VLAN
SERVICES
SYSTEM
More Status
MAIN
Uptime: 0 Days 01:17:12
Host Name: AP
System Time: 12/31/1999 17:17:13
VERSION
FIRMWARE VERSION 2.32 (build 131018)
LOADER VERSION: 2.67 (build 1016)
LAN SETTING
LAN MAC: 04-f0-21-05-79-13
MODE: static
IP ADDRESS: 192.168.168.1
GATEWAY IP ADDRESS :
Pri.DNS IP :
Sec.DNS IP :
LAN cable : Plugged
WAN SETTING
WAN MAC: Not Available
MODE: Not Available
IP ADDRESS: Not Available
GATEWAY IP ADDRESS : Not Available
Pri.DNS IP : Not Available
Sec.DNS IP : Not Available
Radio 1
Wireless Mode: Access Point WDS
LOCAL AP SSID : Antaira Bridge
Frequency: 5.785 GHz
Ack Timeout: 25
MAC: 04-f0-21-05-79-14
LOCAL AP MAC: 04-f0-21-05-79-14
Security: None
Refresh
CONNECTED STATIONS (0)
MAC ADDRESS SIGNAL STRENGTH Tx RATE Tx CCQ Rx RATE CHANNEL WIDTH
LOCAL AP STATISTICS
Bytes Packets Errors
Received: 0 0 0
Transmitted: 0 0 0
LOCAL AP ERRORS
RX Invalid NWID: 2
RX Invalid Crypt : 0
RX Invalid Frag: 0
TX Excessive Retries: 0
Missed Beacons : 0
Other Errors: 0
Select VAP

Navigation

Main Menu Bar

Status: Page displays current status of the device and the statistical information.

Basic Wireless: Page contains the controls for a wireless network configuration, while covering basic wireless settings which define operating mode, associating details and data security options.

Basic Network: Page covers the configuration of network operating mode, IP settings and network services (i.e. DHCP Server).

Advanced Wireless: Page settings for advanced wireless features. Advanced Network page settings for more details of these features.

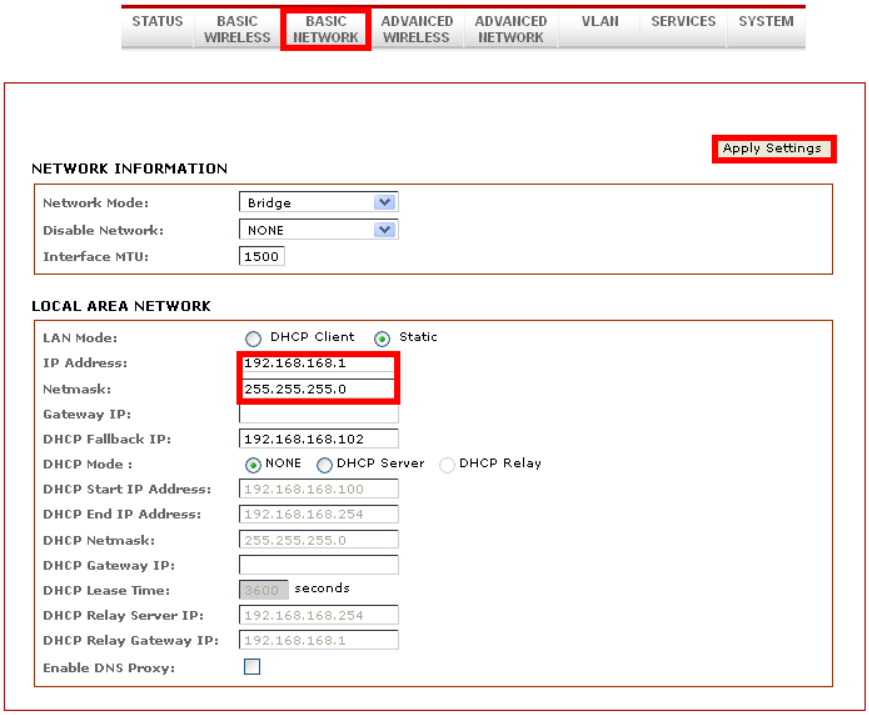
Services: Page covers the configuration of system management services (i.e. Ping Watchdog, Auto-Reboot, SNMP, NTP, Telnet, SSH, System Log).

System: Page contains controls for system maintenance routines, administrator account management, device customization and configuration backup.

Activation Keys: Optional special add-on functions you can purchased separately to activate in device.

Changing the units IP Address

To change the IP address of the unit go to the “Basic Network” tab



This is the user will change the IP address to match their subnet. The “Apply Settings” and “Save” buttons will need to be pressed to finalize the changes.

How to save changes

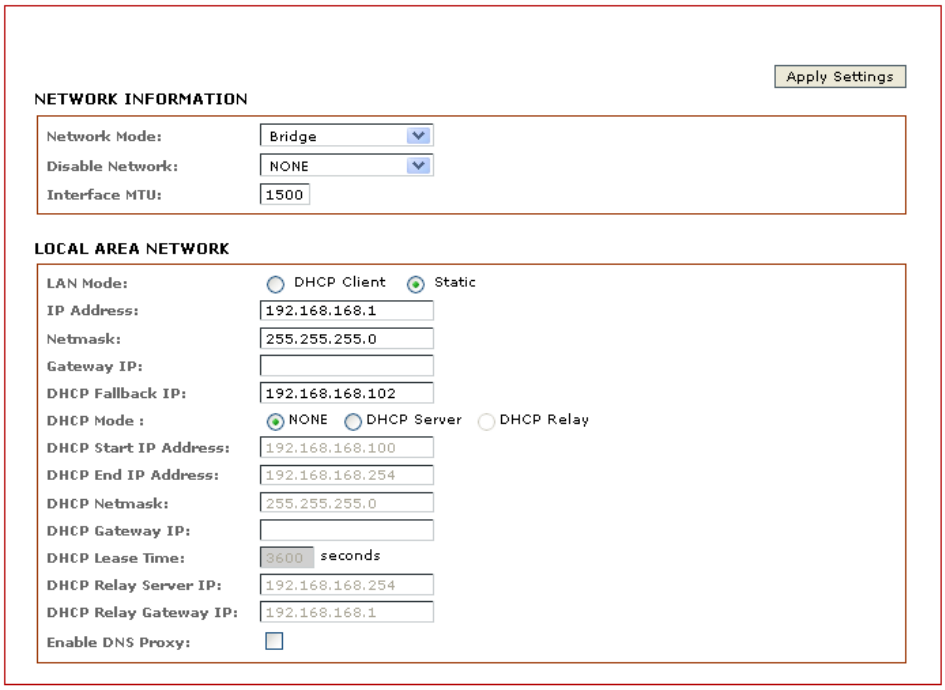
After made changes from each respective setup page, click this button,

Next the prompt below appear.

Click **Save** will write all configuration changes to flash.
Click **Discard** will discard all changes made.
If not sure what changes were made earlier, recommend to discard and reconfigure again.

Basic Network Tab

Click **BASIC NETWORK** from the menu bar to open the page as show below.



Network Mode: Bridging

Network Mode:

Select Bridge mode.

LAN Setup

LAN Mode:

Static: (default) allows the user to enter a specific IP address for the device.
Default IP address is 192.168.168.1

DHCP Client: when set let device learn the IP address automatically from the network.

Netmask:

Allows the user set the class for the IP address set.
Default value is 255.255.255.0

Gateway: (optional)

Enter the gateway IP address of the network the device is connected.

Primary DNS IP: (optional)

Enter the primary DNS IP address nearest to the gateway router.

Secondary DNS IP: (optional)

Enter the secondary DNS IP address nearest to the gateway router.

DHCP Mode:

None: function disabled

DHCP Server: Check to enable. Device act IP address distribution server automatically issue IP address and other network information to the DHCP Client request them.

DHCP Relay: check to enable. Enter the IP address of the remote DHCP server where the DHCP Client request will be relayed to.

DHCP Start IP Address:

Enter the starting IP address to be issue.

DHCP End IP Address:

Enter the last IP address the server will issue.

Netmask:

Allows the user to set the IP class for the IP address range set for the start and end address.

DHCP Lease Time: (default is **3600** seconds or 1hour)

Enter the new lease time in seconds.

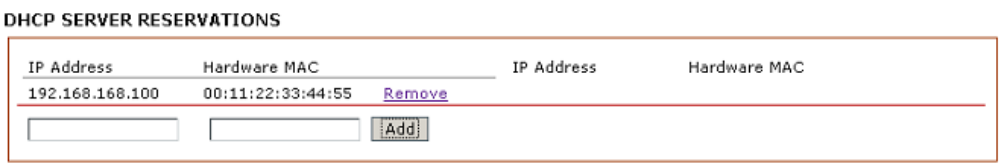
DHCP Server Relay IP:

Enter the IP address of the remote DHCP server where the DHCP Client request will be relay to get the IP address.

DHCP Gateway Relay IP:

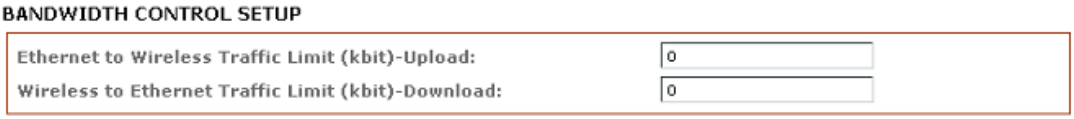
Enter the IP address of the remote gateway where the DHCP Client request will be relay to get the gateway IP address.

DHCP Reservations



Click **Add** to enter for each device the IP address and MAC address.
All DHCP active lease devices are displayed in the **Status** tab page from the **More Status** selection.

Bandwidth Control between Ethernet and Wireless



An entry of value “0” means no bandwidth flow limit between the 2 interfaces.
An entry of “2000” means 2000Kbit or 2Mbit limit traffic flow between the 2 interfaces.
Default is “0”

Basic Wireless Tab

Under the tab, there is the selection of 4 radios.

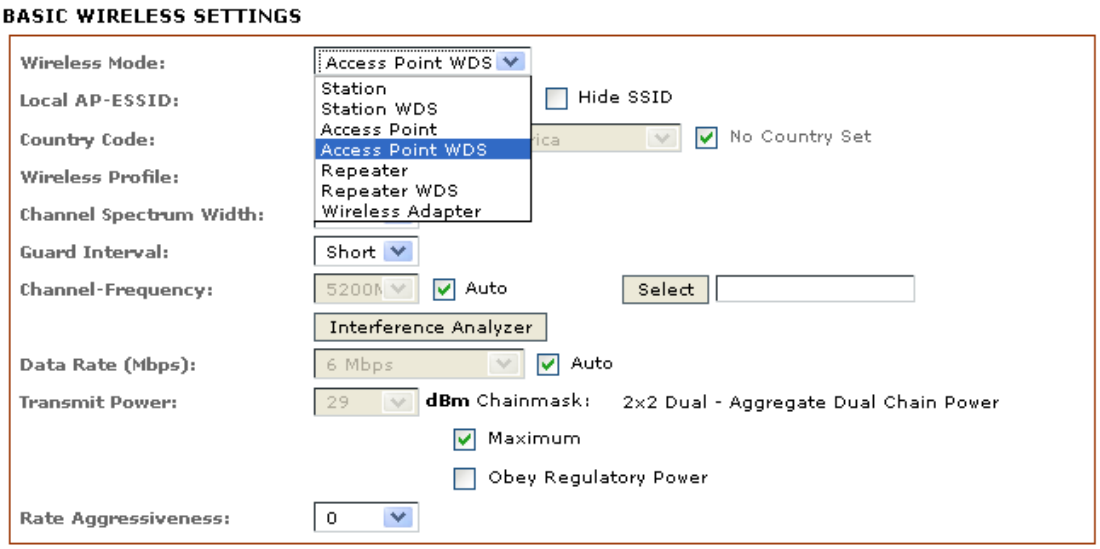
Fig 2.1 Basic Wireless Tab

Currently device support only one 802.11n radio card. Select **RADIO 1** to configure. Basic Wireless Tab contains all the wireless setup, which is necessary for the operator to setup the wireless part of the link.

Basic Wireless Settings

All the basic wireless settings can be configured in this page. Operators can change the ESSID, regulatory country code, wireless profile, channel spectrum width, frequency of interest, data rates, transmit power and rate aggressiveness.

Wireless Mode



Access Point

This mode can be connected to **Station** mode, and then forwards all the traffic to the network devices connected to the Ethernet devices of the Station.

Access Point WDS

This mode can be connected to Station WDS mode. Using WDS protocol, it allows a client or station device to bridge wireless traffic transparently.

Station:

This is a client mode that can be connected to the Access Point mode. It is used to bridge the wireless connection to an Access Point. It forwards all the traffic to/from the network devices to the Ethernet interface. This mode translates all the packets that pass through device to its own MAC address, thus resulting in a lack of transparency.

Station WDS

WDS is the acronym of Wireless Distribution System. It can be connected to the **Access Point WDS** mode. It enables packet forwarding at layer 2 level. Unlike Station mode, it is fully transparent at layer 2 level.

****Note:- for Station WDS, Access Point WDS, Repeater WDS:**
WDS protocol used is not defined as the standard, thus compatibility issues between equipment from different vendors might arise.

Repeater WDS

This mode consists of a Station WDS and an Access Point WDS mode. The Repeater WDS must first link up with an Access Point WDS, and then it can link up with a Station WDS. It acts as an extension to the link and can add more Repeater WDS as necessary.

***Note:- for Repeater WDS:**
ESSID must be the same for the Remote AP and the Local AP. The channels used Repeater to link to another Repeater will follow the Access Point WDS connection selected channel.

Access Point Parameters Settings

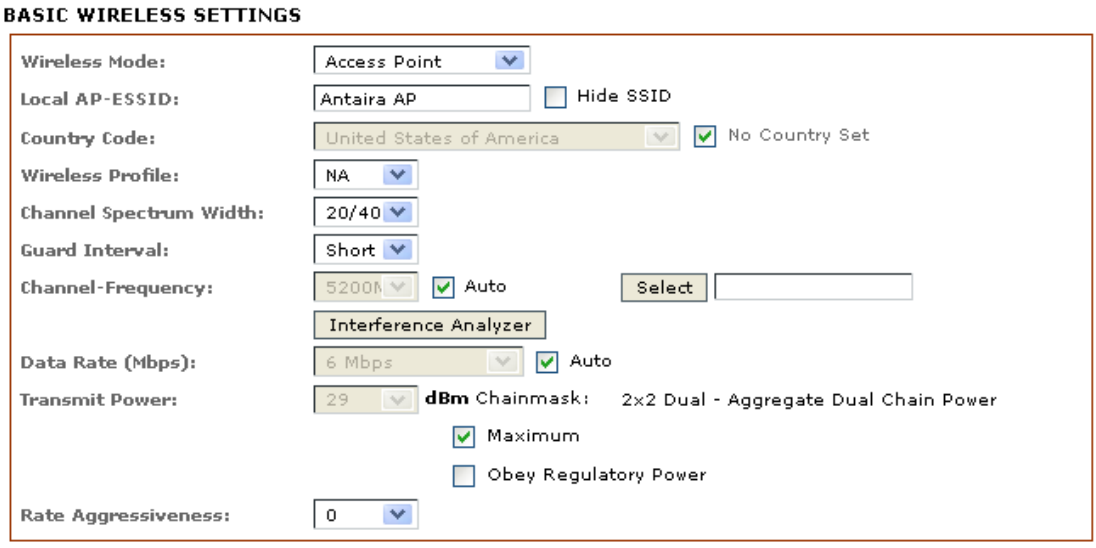


Fig 2.3 Basic Wireless Settings (Access Point/ Access Point WDS)

Local AP-ESSID

This is the Service Set Identifier used to identify the operator's wireless LAN. It should be specified while operating in **Access Point** or **Access Point WDS mode**.
All the client devices within its range will receive broadcast messages from the access point advertising this SSID.

Hide SSID*:*
Once checked, this will disable advertising the SSID of the access point in broadcast messages to wireless stations. This option is only available in Access Point, Access Point WDS and Repeater WDS mode only.

Country Code

Different countries have different power levels and frequency selections. To ensure device operation follows regulatory compliance rules, operator to select correct country code where device will be used. The channel list, output power limits, IEEE 802.11 and Channel-Spectrum Width modes will be tuned according to regulations of the selected country.

No Country Set*:*

Option when checked, only the frequency range are available.
11n 5GHz is 5180-5320MHz and 5745-5825MHz.

Wireless Profile:

NA is 11n 5GHz band and represents a mixed of 802.11n and 802.11a mode.

Channel Spectrum Width

20M represents the data transmitted at a bandwidth of 20MHz. 20/40MHz represents the data transmitted at either 20MHz or 40MHz. In very noisy environment it automatically falls back to 20MHz to be more resilient to the interference. In situation when auto fall back did not happened, manually changing channel spectrum width to 20MHz will to help reduce interference on the link and improve performance.

*** Note: 40MHz bandwidth is non-standard for 802.11n/g mode operation. If you experience unstable performance change Channel Spectrum Width to 20M.**

Channel – Frequency

This is frequency selection the user can set for device to operate on. The frequency range available depends on the country domain you select in Country Code. For 5GHz frequency range some have DFS characteristics earmarked by regulations. Selecting one of these frequencies for operation may affect and delay of 2 minutes or more (possibly up to 10 minutes in some situations) for device to attempt to establish a connection.

Auto*:* When checked, during startup, device automatically selects the least interfering channels (or frequency) for the operation.

Data Rate

Data Rates consist of both the legacy rates and the MCS (Modulation Coding Scheme – Only for 802.11n) rates.

6 – 54Mbps are Legacy Rates

MCS0 to MCS7 are 802.11n rates, which uses only 1 stream.

MCS8 to MCS15 are 802.11n rates, which uses 2 streams.

Auto*:* The data rate selected will follow an advanced rate algorithm that takes into condition the amount of errors at the data rate and fine tune to the best data rate it can use.

Transmit Power

The maximum transmit power displayed is determined by the country code and the maximum transmit power of the miniPCI that is being used.

Note on changing channels:

When the operator changes the channels and if this new frequency have higher power output permitted by regulation, the power previously selected low power level will remains unchanged. The user needs to readjust the power level to in order to take advantage higher output power available for the channel

.

Rate Aggressiveness

Allows user to reduce or increase transmit rate while still remain in Fully Auto Algorithm. There are 2 scenarios that Rate Aggressiveness is useful. Environment might be noisy at times. Lower the throughput will ensure better stability. Rate Aggressiveness allows device to reduce the transmit rate, so range or power can be higher.

Choose a range of value from -3, -2, -1 Environment might be free of interference. But the fully auto algorithm might give low throughput. Increase Rate Aggressiveness will increase transmit rate in this case to get higher throughput. Choose a range of value from +3, +2, +1.

Station Parameters Settings

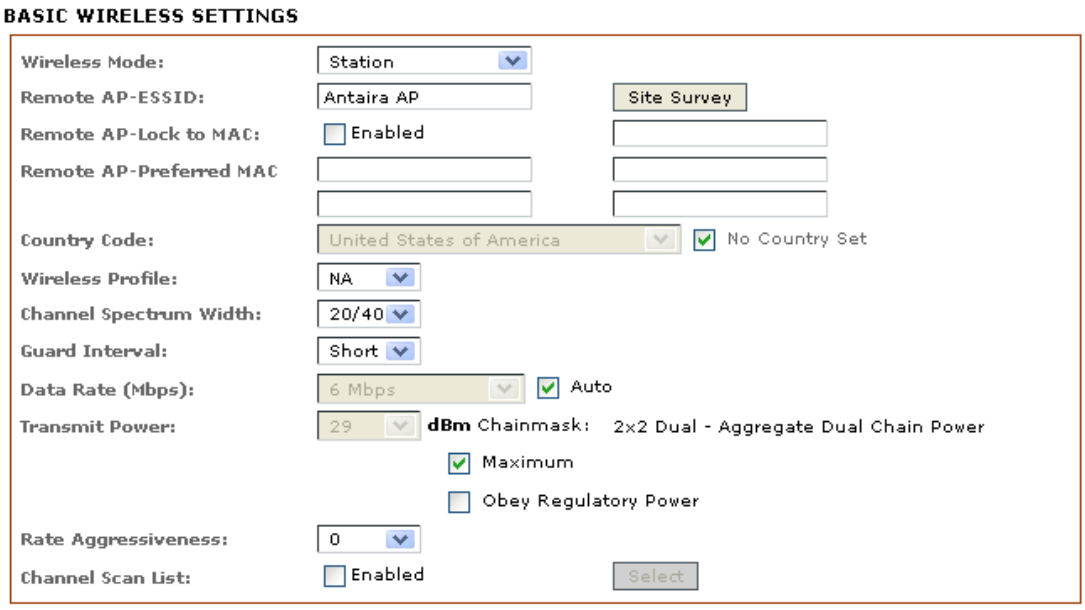


Fig 2.4 Basic Wireless Settings (Station/Station WDS)

These options below are only available in **Station, Station WDS** and **Repeater WDS** modes unless otherwise stated.

Wireless Mode: Station

Remote AP-ESSID

This is the Service Set Identifier used by station to seek and connect to the access point of same the SSID identifier.

Site Survey

Site Survey will search for the available wireless networks in range on all the supported channels and will allow you to select one for association. In case the selected network uses encryption, you'll need to set security parameters in wireless security section. Click Scan to re-scan the Access Points in range. Select the Access Point from the list and click Close this window. Site Survey channel scan list can be modified using the Channel Scan List control.

Remote AP – Lock to MAC

Enter the MAC address of the remote access point the device is connected to. This option will make device only connect to this access point. This is important when connection is Point-to-Point operation.

Remote AP - Preferred MAC

Enter the preferred MAC address of the access point you want device to connect when it first startup. Up to max of 4 MAC addresses can be entered. Priority is from top to bottom. In the event all preferred MAC addresses are not available, device will then pick the matching SSID access point with the strongest signal.

Country Code

Different countries have different power levels and also frequency selections. To ensure device operation follows regulatory compliance rules, the operator should make sure that correct country code where device will be used, is selected. The channel list, output power limits, IEEE 802.11 and Channel Spectrum Width modes will be tuned according to the regulations of the selected country. **Station setting must match AP country code setting.**

No Country Set*:*

Option when checked, only the frequency range are available.
11n 5GHz is 5180-5320MHz and 5745-5825MHz.

Wireless Profile:

NA is 11n 5GHz band and represents a mixed of 802.11n and 802.11a mode.

** **Station setting must match AP Wireless Profile setting.**

Channel Spectrum Width

20M represents the data transmitted at a bandwidth of 20MHz. 20/40MHz represents the data transmitted at either 20MHz or 40MHz. In very noisy environment it automatically fall back to 20MHz to be more resilient to the interference. In situation when auto fall back did not happened, manually changing channel spectrum width to 20MHz will to help reduce interference on the link and improve performance.

*** Note: 40MHz bandwidth is non-standard for 802.11n/g mode operation. If the user experiences unstable performance change Channel Spectrum Width to 20M.**

** **Station setting must match AP Channel Spectrum Width setting.**

Maximum : checking this box will result in maximum Tx output power overriding regulation.

Obey Regulatory Power : checking this box will obey Tx output regulatory power by country.

Channel Scan List

By checking the “Enabled” button the operator can chose a specific channel.

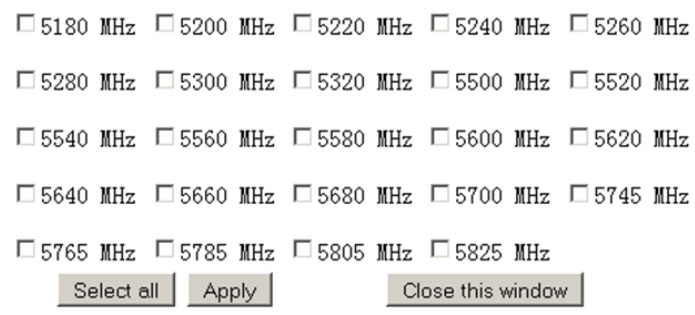


Fig 2.5 Channel Scan List (In US Country Code)

According to the availability of channels in the country codes, the operator can select which channels to be scanned when scanning for an Access Point. Then the scanned channels will appear on the Site Survey.

Wireless Security

All the wireless security settings are set under this section.
The operation of the Keys is the same for ALL the Wireless modes.

WPA or WPA2 Authentication

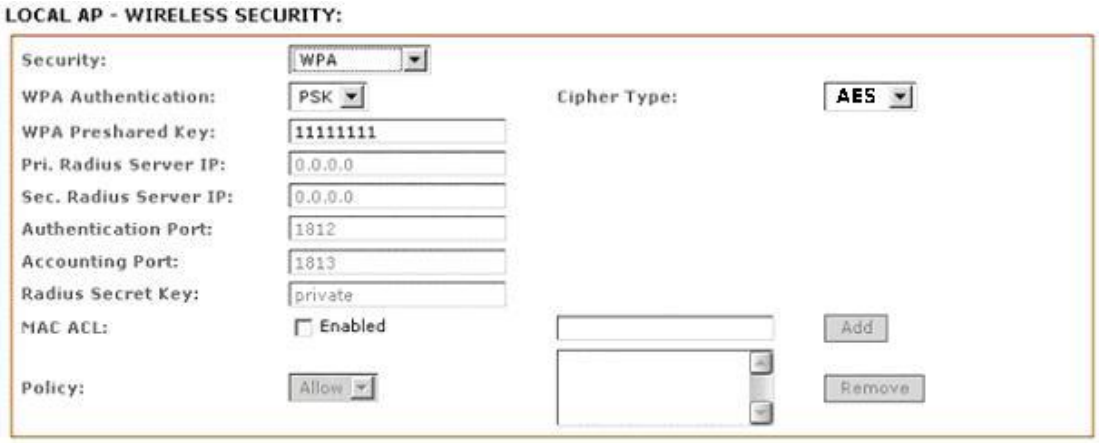


Fig 2.7 WPA (Access Point/Access Point WDS/Repeater WDS)

WPA PSK

PSK (Default) – WPA or WPA2 with Pre-shared Key method.

Cipher Type

TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.

AES - Advanced Encryption Standard (AES) algorithm.

AUTO (Default) – Automatically select between both algorithms.

Preshared Key

This option is available when **WPA** or **WPA2**, with **PSK** selected.

The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

***** Important:**
802.11n network using WPA authentication should use AES cipher type for connection. Only AES allows highest transmission speed and throughput operation.
Using TKIP cipher type device will limit maximum transmission speed of up to 54Mbps only.

WPA + EAP

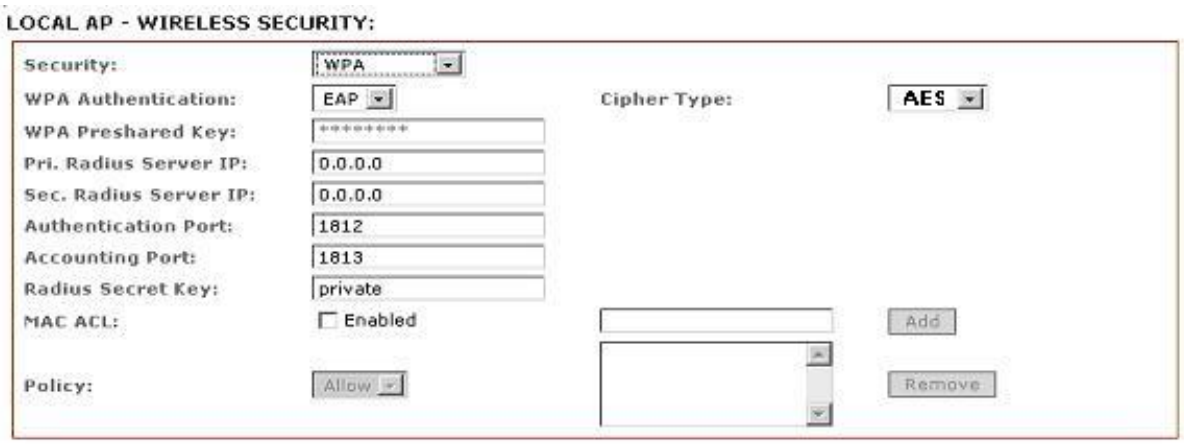


Fig 2.8 WPA + EAP

EAP – WPA or WPA2 with EAP (Extensible Authentication Protocol)

Firmware supported options for clients are: EAP-TTLS and EAP-PEAP

Cipher Type

TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.

AES - Advanced Encryption Standard (AES) algorithm.

AUTO (Default) – Automatically select between both algorithms.

Primary Radius Server IP

Enter the Primary Radius Server IP address.

Secondary Radius Server IP

Enter the Secondary Radius Server IP address.

Authentication Port

Enter the Authentication Port number of the Radius Server. Default is 1812.

Accounting Port

Enter the Accounting Port number of the Radius Server. Default is 1813.

Radius Secret Key

Enter the Secret Key of the Radius Server. The device uses this to authenticate itself with Radius Server.

WPA EAP-TTLS and WPA EAP-PEAP

Fig 2.8 WPA (Station /Station WDS/Repeater WDS)

This applies to the following modes only, when **WPA** or **WPA2**, with **EAP** is selected.

Station, Station WDS, Repeater WDS Mode

Identity

Identification credential used by the wpa-supplicant for EAP authentication.

User Name:

Identification credential used by the wpa-supplicant for EAP tunneled authentication in unencrypted form.

User Password:

Password credential used by the wpa-supplicant for EAP authentication

IEEE802.1x Settings

The operation of the Keys is the same for ALL the modes.

**** Note: Operating with IEEE802.1x security will limit AP to maximum wireless link speed of 54Mbps only.**

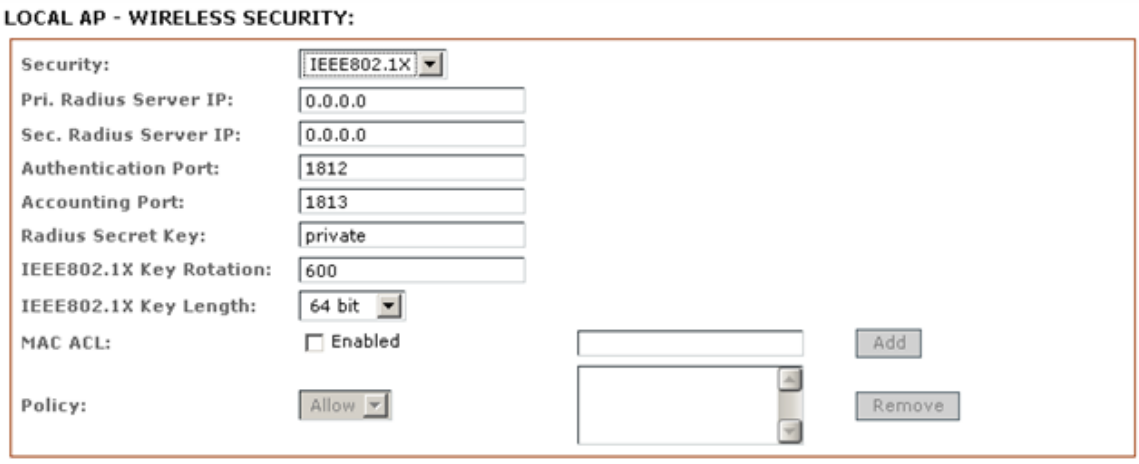


Fig. 2.8 IEEE802.1X (Access Point/Access Point WDS/ Repeater WDS)

This option apply to the following modes only, when WPA EAP or IEEE802.1x .

Access Point, Access Point WDS, Repeater WDS modes

Primary Radius Server IP

Enter the Primary Radius Server IP that Access Point will use to query server.

Secondary Radius Server IP

Enter the Secondary Radius Server IP that Access Point will use to query the server.

Authentication Port

Enter the Radius Server Authentication Port number to use. Default is 1812.

Accounting Port

Enter Radius server Accounting Port to use. Default is 1813.

Radius Secret Key

Enter Radius server Secret Key that Access Point to use to authenticate itself with radius server.

IEEE802.1x Key Rotation

Enter time in seconds. Time before activate key rotation in authentication process for higher security.

IEEE802.1x Key Length

This is the key length of the initial seed key. Select 64 or 128bit.

WEP

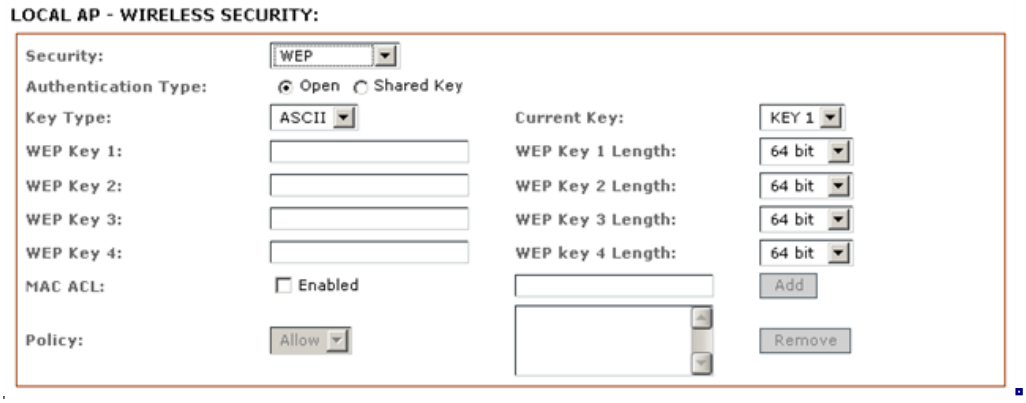


Fig 2.6 WEP

The operation of the Keys is the same for ALL the modes.

**** Note: Operating with WEP security will limit AP to maximum wireless link speed of 54Mbps only.**

Authentication Type:

Open Authentication – (Default) No authentication. Recommend to use this standard option over shared authentication.

Shared Authentication – May not be compatible with all Access Point. Not recommended.

Key Type:

HEX or **ASCII** option specifies the character format for the WEP key if WEP security method is used.

Current Key:

Specify the Index of the WEP Key used. 4 different WEP keys can be configured at the same time, but only one is used.

WEP Key:

WEP encryption key for the wireless traffic encryption and decryption should be specified if WEP security method is used.

WEP Key Length:

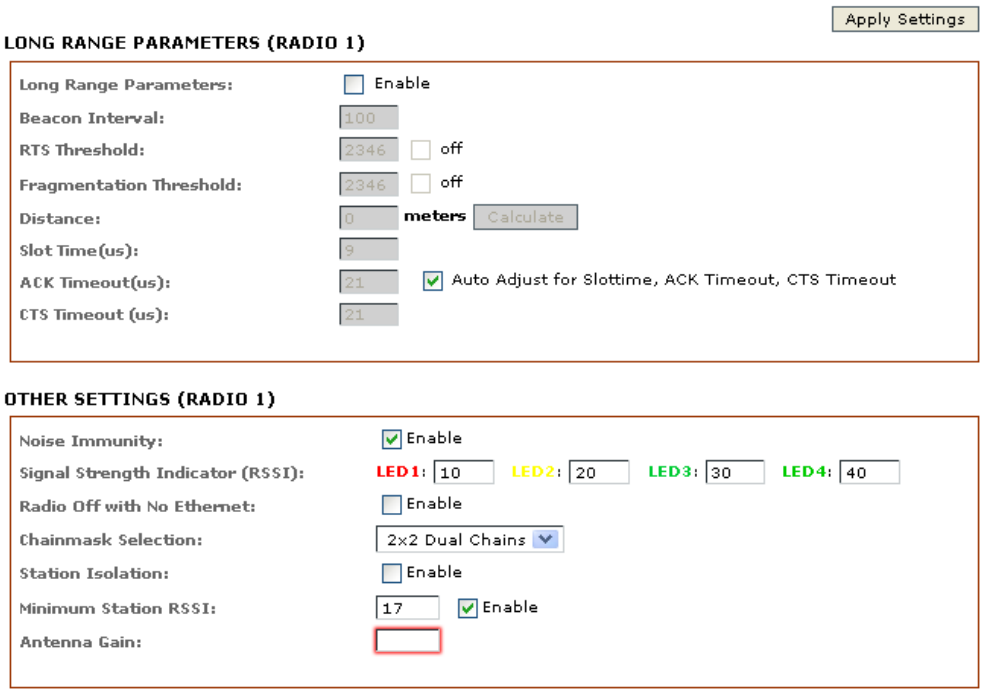
64-bit (selected by default) or 128-bit WEP Key length should be selected if WEP security method is used. The 128-bit option will provide higher level of security.

For **64-bi**t – specify WEP key as 5 HEX (0-9, A-F or a-f) pairs (e.g. 00112233AA) or 5 ASCII characters.

For **128-bit** – specify WEP key as 13 HEX (0-9, A-F or a-f) pairs (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

Advance Wireless Tab

Click **Advanced Wireless** tab from menu and select **RADIO 1** to open the page below.



Long Range Parameters Setup

Advanced wireless page let you setup outdoor long distant connection parameters.

Long Range Parameters:

Check to enable parameters.

Beacon Interval: (default is 100 ms)

Define the time interval (in millisecond) the beacon to broadcast.

Recommend to use default.

RTS Threshold: (Default is **OFF**)

Fragmentation Threshold: (Default is **OFF**)

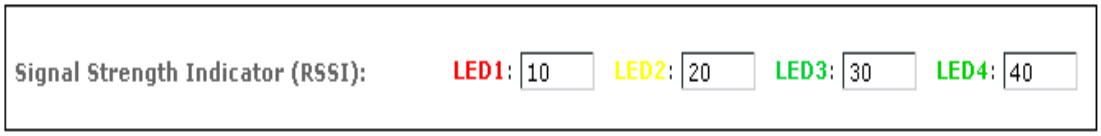
Distance:

Enter the distant in meters the device is to connect with the opposite device. Then click **Calculate.** The close approximate values for Slot Time, ACK Timeout, CTS Timeout will be calculated. Fine tuning can be further adjusted for the best environment conditions to achieve best performance and better link reliability.

Noise Immunity:

Check to enable. When enabled, it automatically adjusts the signal/noise level for best performance. In low noise environment it is recommended to turn off this function.

Signal Strength Indicator (RSSI):



The default values are LED1-Red (10), LED2-Yellow (20), LED3-Green (40) Each LEDs when turn on indicates the RSSI signal strength has hit over the value. e.g. When LED1 and LED2 light up it indicate the RSSI is greater than 20.
When all 4 LEDs light up it indicate RSSI is greater than 40.
For long distant installation when signal strength expected to be about 20-30, the values can be adjusted to display over this new range.
e.g. the LEDs values can be adjusted as follows:

LED1 (RSSI value=7)
LED2 (RSSI value=15)
LED3 (RSSI value=22)
LED4 (RSSI value=27)

Station Isolation:

When checked, prevent wireless clients on same AP from discovering other clients.

Chainmask Selection:

Available selections are: a) **1x1 Left Chain**, b) **1x1 right Chain** and c) **2x2 Dual Chain**

Selecting **1x1 Left Chain** will forced radio card to operate with 1transmit and 1 receive stream and both transmit /receive on the left port of radio card only.

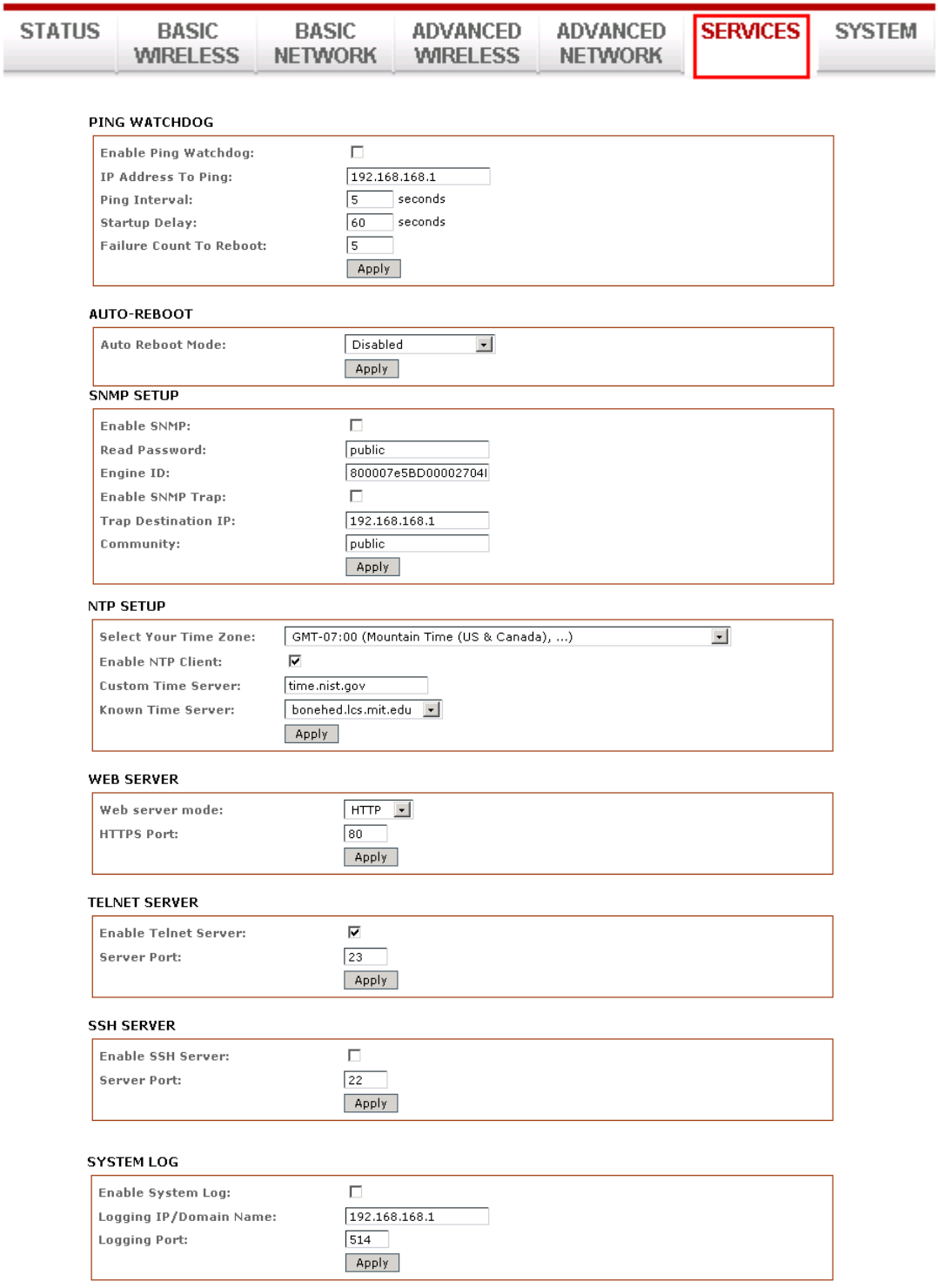
Selecting **1x1 Right Chain** will forced radio card to operate with 1 transmit and 1 receive stream and both transmit /receive on the right port of radio card only.

Selecting **2x2 Dual Chain** (default) will enable radio card to operate with 2 transmit and 2 receive streams and automatically transmit /receive on any of the 2 radio card ports.

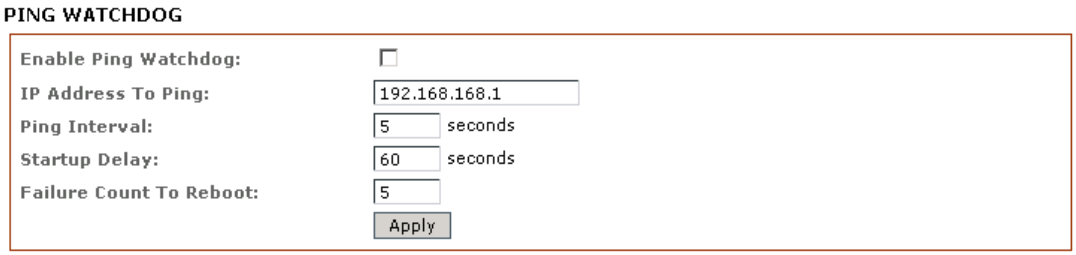
Services Tab

Click **Services** tab from menu to open the page below.

Services section provides varieties of useful and enhanced functions to help assist device operations.



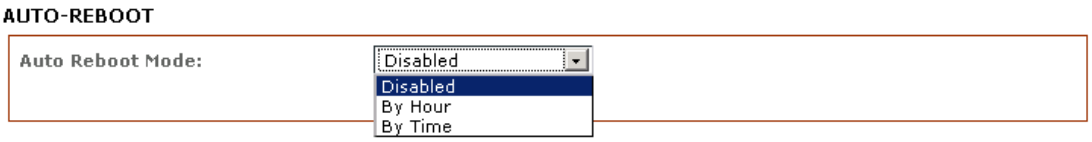
Ping Watchdog



Enable Ping Watchdog: Default is disabled. Check on box to enable.

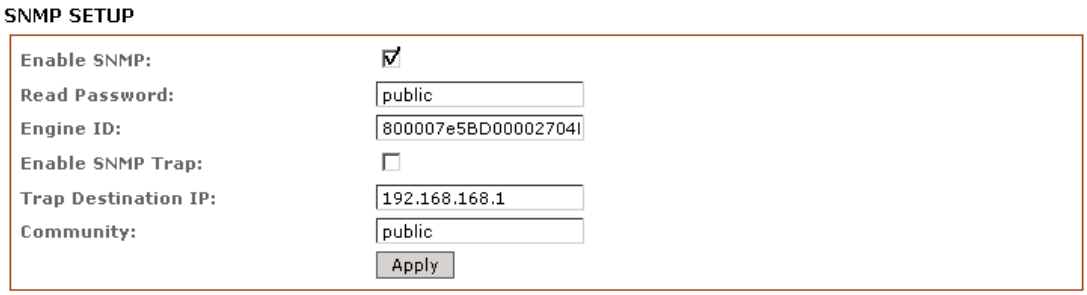
IP Address To Ping: Target IP address do ping test monitor.
Ping Interval: Default is 5 seconds (minimum). This is Ping test duration.
Startup Delay: Default is 60 seconds(minimum).
One time delay after device startup.
Failed Count To Reboot: Default is 5. This is the number of ping failure count before device kick in the reboot process.

Auto-Reboot



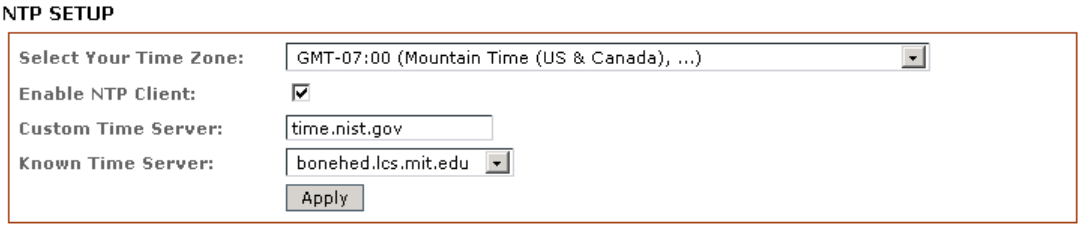
Auto-Reboot Mode: Default is disabled. Select by Hour or by Time check. This mode lets you preset a timer to automatically force a reboot. Timer can in fixed number of hours or at a specified time of day.
By Hour: Enter the number of hours device need to run before kick start reboot process.
By Time: Enter the specific time of day in hh:mm (24-hour format) to kick start reboots process.

SNMP Setup



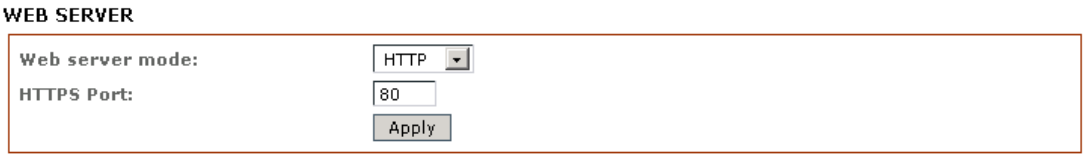
Enable SNMP: Default is disabled. Check on box to enable.
Read Only Password: Password to query device.
Engine ID: Default is 800007e5BD00002704D000007c
Enable SNMP Trap: Default is disabled. Check on box to enable.
Trap Destination IP: Enter the IP to send the info when trap is triggered.
Community: Enter the SNMP community string.

NTP Setup



Enable NTP Client: Default is disabled. Check on box to enable.
Select Your Time Zone: Select from list the country you reside.
Custom Time Server: Default is “time.nist.gov“ Enter preferred time server domain/IP
Known Time Server: The user can also select one from this list as the new time server.

Web HTTP Security



Web Server Mode: Default is HTTP. Option is HTTP and HTTPs
HTTP(s) Port: Default is 80 for HTTP and 413 for HTTPs.
Enter a new preferred port number.

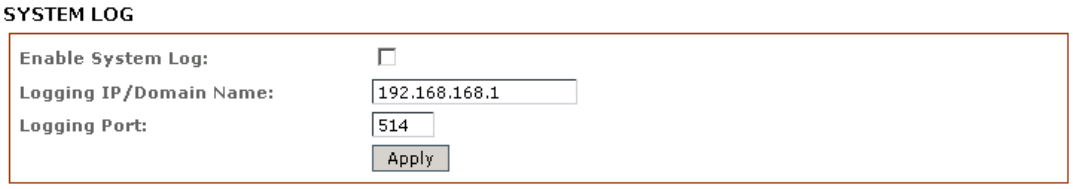
Telnet Access Setup

Enable Telnet Server: Default is enabled. Remove check on box to disable.
Server Port: Default is 23. Enter new preferred port number.

SSH Access Setup

Enable SSH Server: Default is disabled. Check on box to enable.
Server Port: Default is 22. Enter new preferred port number.

System Log Setup

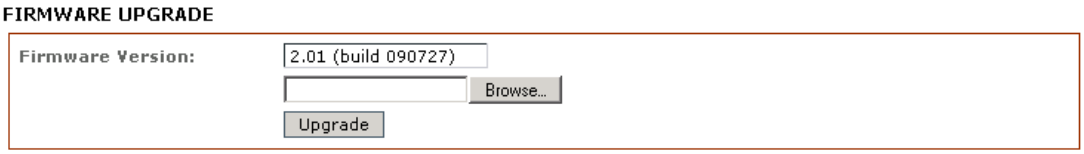


Enable System Logging: Default is disabled. Check on box to enable.
Logging IP /Domain Name: Enter destination IP address of device to receive log.
Logging Port: Default is 514. Enter the new preferred port number.

System Tab

The System Page contains Administrative options. This page enables administrator to customize, reboot the device, set it to factory defaults, upload a new firmware, backup or update the configuration and configure administrator's credentials.

Firmware Upgrade



Use this section to find out current software version and update the device with the new firmware. The device firmware update is compatible with all configuration settings. System configurations are preserved while the device is updated with a new firmware version.

Firmware version: displays the version of the current firmware of the device system.

Upgrade: button opens the Firmware Upload window if activated.

Current Firmware: displays the version of the device firmware which is currently operating.

Firmware File: activate Browse button to navigate to and select the new firmware file. The full path to the new firmware file location can be specified there. New firmware file is transferred to the system after Upload button is activated.

Close this window – button cancels the new firmware upload process if activated.

Upgrade button: should be activated in order to proceed with firmware upgrade routine (new firmware image should be uploaded into the system first). Please be patient, as the firmware upgrade routine can take 3-7 minutes. The based device will be un-accessible until the firmware upgrade routine is completed.

Do not switch off, do not reboot and do not disconnect the device from the power supply during the firmware upgrade process as these actions will damage the device!

It is highly recommended to backup the system configuration and the Support Info file before uploading the new configuration.

Close this window – button closes the firmware upgrade window if activated.
This action will not cancel the firmware upgrade process.

Host Name

Host Name is the system wide device identifier. It is reported by SNMP Agent to authorized management stations..

Host Name: specifies the system identity.

Change button: saves the Host Name if activated.

Administrative and Read-only Account

In this section the user can modify the administrator password to protect the device from unauthorized configuration. The default administrator's password should be changed on the very first system setup:

Administrator Username: specifies the name of the system user.

Current Password: administrator is required to enter a current password. It is required for Password or Administrator Username change routine.

Default administrator login credentials:

- User Name: **admin**
- Password: **password**

New Password: new password used for administrator authentication should be specified.

Verify Password: new password should be re-entered to verify its accuracy.

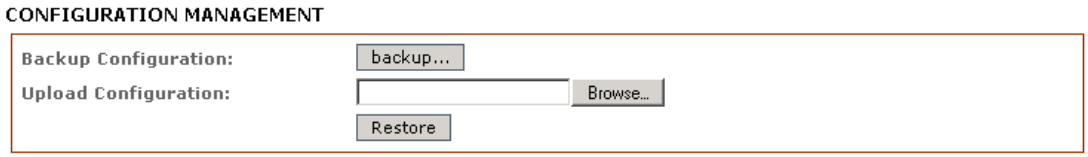
Click Change button to save the changes.

Enable Read-Only Account

Read-Only Username

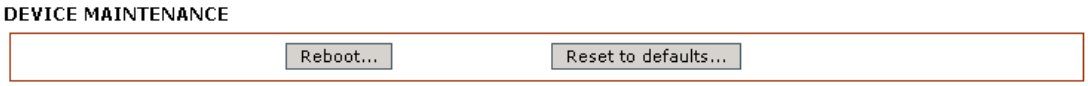
Password: new password used for read-only administrator authentication should be specified.

Configuration Management



Backup Configuration: click Download button to export the current configuration to a file.
Upload Configuration: click Browse button to navigate to and select the new configuration file or specify the full path to the configuration file location.
Activating the Upload button will transfer new configuration file to the system.
New configuration will be effective after the Apply button is activated and system reboot cycle is completed. Previous system configuration is deleted after Apply button is activated. It is highly recommended to backup the system configuration before uploading the new configuration.
Use only configuration backups of the same type device.

Device Maintenance



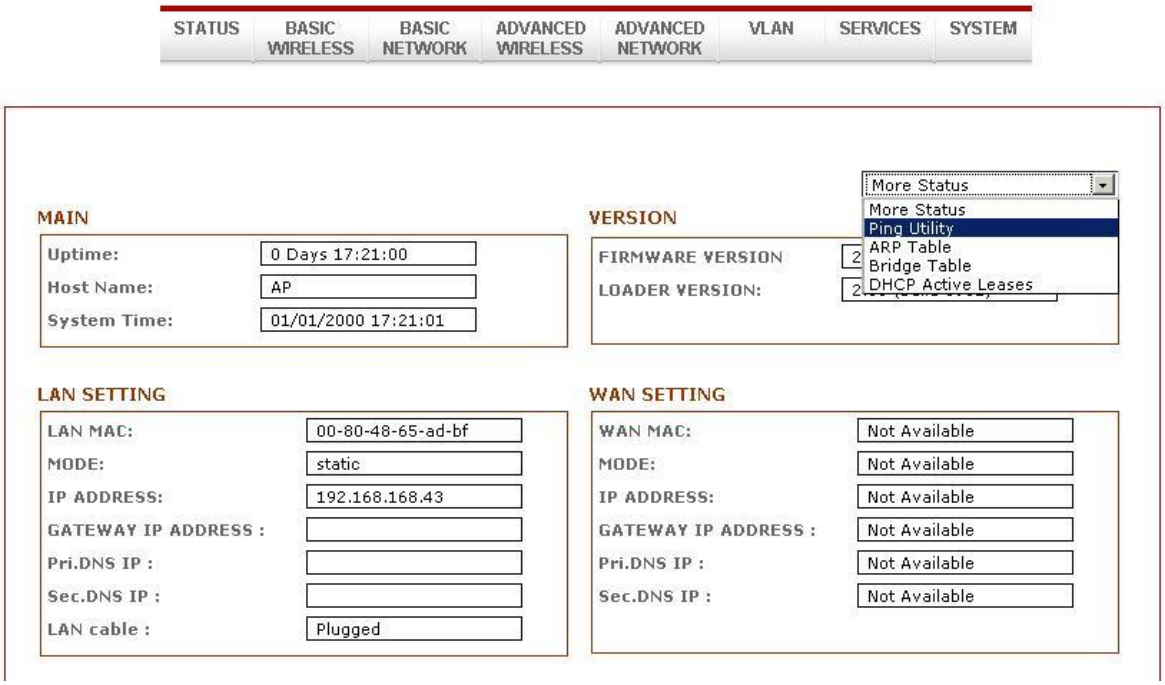
The controls in this section are dedicated for the device maintenance routines: rebooting, resetting, generating of the support information report.

Reboot: activate Reboot control in order to initiate full reboot cycle of the device. Reboot effect is the same as the hardware reboot which is similar to the power off - power on cycle. The system configuration is not modified after the reboot cycle completes. Any non-applied changes will be lost.

Reset to Defaults: activate Reset to Defaults control in order to initiate reset the device to factory defaults routine. Reset routine initiates system Reboot process (similar to the power off - power on cycle). The running system configuration will be deleted and the default system configuration (all the system settings with no exception) will be set.

After the **Reset to Defaults** routine is completed, the device system will return to the default IP configuration (192.168.168.1/255.255.255.0) and will start operating in Station-Bridge mode. It is highly recommended to backup the system configuration before the Reset to Defaults is initiated.

Status Page



The Status Page displays a summary of link status information, current values of basic configuration settings (depending on operating mode), network settings and traffic statistics of all the interfaces.

Status Reporting

Main

Uptime: displays device up time since boot up. The time is expressed in days, hours, minutes and seconds.
Host Name: displays the assigned device host name (ID).

System Time: display device current date and time. Accurate system date and time is retrieved from the internet services using NTP (Network Time Protocol) if device is setup and connected to internet. Otherwise, the date and time update from device own inaccurate autonomous clock.

Version Firmware Version: displays current firmware version in operation.
Loader Version: displays current loader version of the device.

LAN Setting

LAN MAC: displays the MAC address of the device LAN (Ethernet) interface.
LAN Mode: displays the mode used, either static or DHCP client.
LAN IP Address: displays the current IP address of the LAN (Ethernet) interface.
LAN Gateway IP Address: displays the IP address of the gateway used in LAN.
LAN Primary DNS IP: displays the Primary DNS IP address of the LAN setting.
LAN Secondary DNS IP: displays the Secondary DNS IP address of the LAN setting.

WAN Setting

WAN MAC: displays the MAC address of the device WAN interface.
WAN Mode: displays the mode used, either DHCP, PPPoE or Static IP.
WAN IP Address: displays the current IP address of the WAN interface.
WAN Gateway IP Address: displays the IP address of the gateway used in WAN.
WAN Primary DNS IP: displays the Primary DNS IP address of the WAN setting.
WAN Secondary DNS IP: displays the Secondary DNS IP address of the WAN setting.

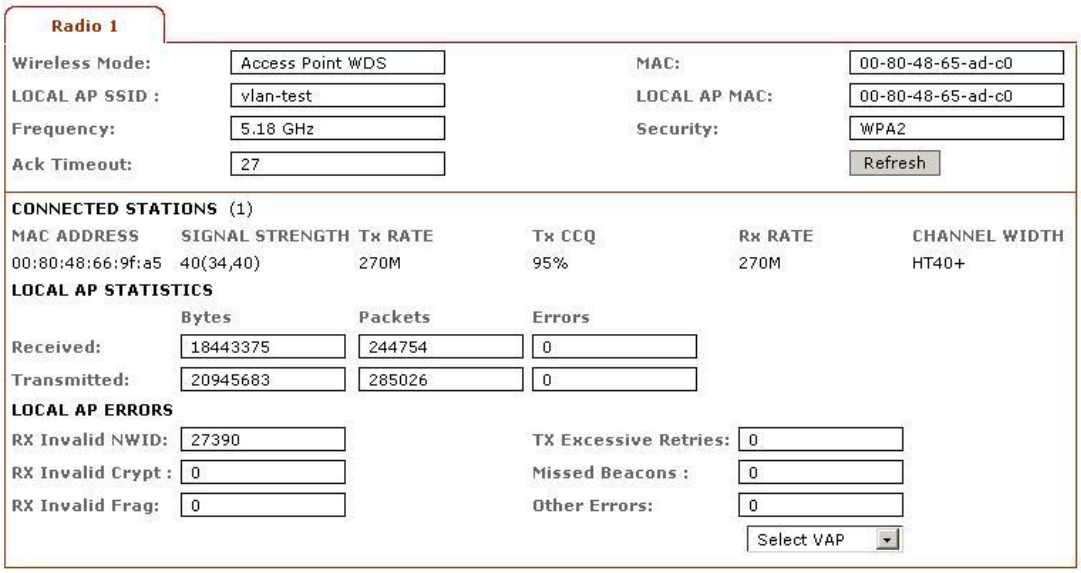
Radio

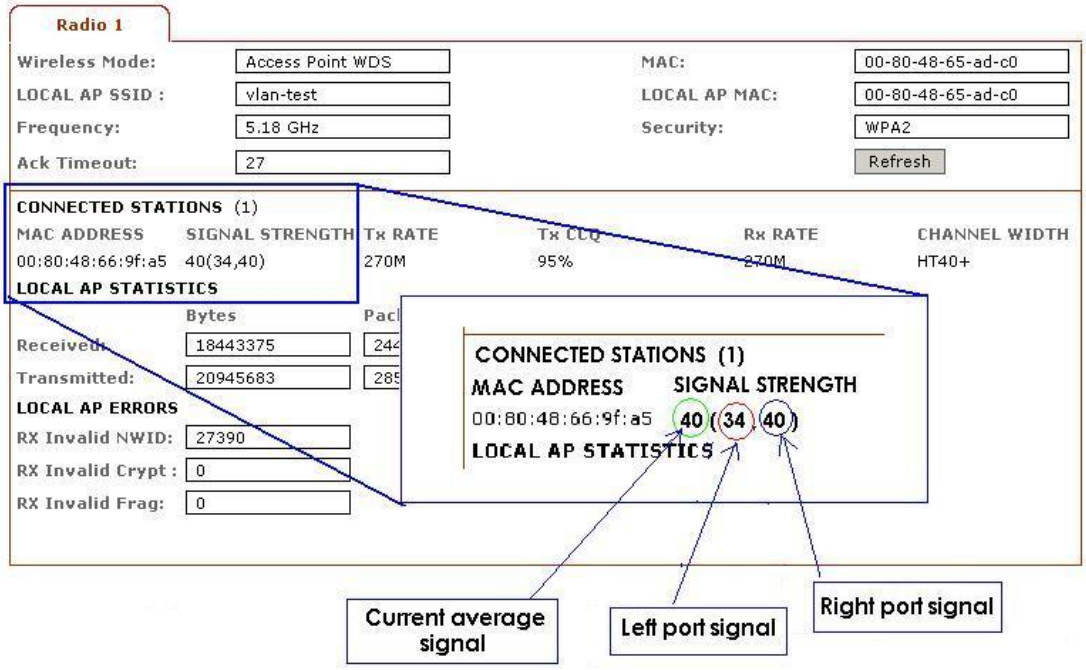
Wireless Mode: displays the current operating mode of the device.
Local AP SSID: displays the current SSID (Service Set Identifier) of device when operates in access point mode.
Frequency: displays current operating frequency running in device.
WLAN MAC: displays the MAC address or BSSID of the current active WLAN card running in device.
WLAN Local/Remote AP MAC: displays the MAC address of the WLAN card connected to it.
WLAN Security: display the current active security mode.

Clients Connection Status in AP Status Info

All clients connected to AP can be view from AP Status page.
Below is an example of a client's connection status info.

Click Refresh to refresh client connection statistics and status page



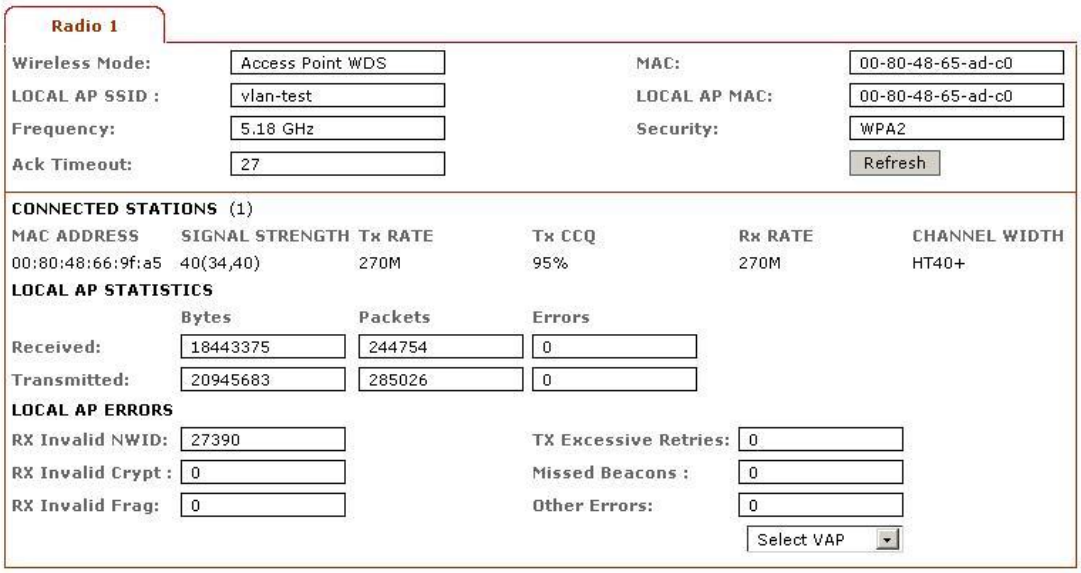


Signals strength at the left and right port of radio card can be view with more accurately while adjusting the antenna to get a more balanced reception.

Station Connection Info

Status Info

Click Refresh to refresh client connection statistics and status page.



WLAN Connected Status:

MAC Address: displays the MAC address of the current active WLAN card.

Signal Strength: displays the received wireless signal level of opposite connected device.

TX Rate and RX Rate: displays the current 802.11 data transmission (TX) and data reception (RX) rate while operating in Station mode. Typically, the higher the signal and the higher the data rate the higher the data throughput will be.

Channel Width: HT20 indicates established connection is 20MHz channel width
HT40+ indicates established connection is 40MHz channel width

WLAN Local AP Statistics:

Bytes transmitted/received value represents the total amount of data (in bytes) transmitted and received during the connection;

WLAN Local AP Errors: section displays the counters of 802.11 specific errors which were registered on wireless interface:

Rx invalid NWID value represents the number of packets received with a different NWID or ESSID - packets which were destined for another access point. It can help to detect configuration problems or identify the adjacent wireless network existence on the same frequency.

Rx Invalid Crypt value represents the number of transmitted and received packets which were encrypted with the wrong encryption key and failed the decryption routines. It can be used to detect invalid wireless security settings and encryption break attempts.

Rx Invalid Frag value represents the number of packets missed during transmission and reception. These packets were dropped due to re-assembling failure as some link layer fragments of the packet were lost.

Tx Excessive Retries value represents the number of packets which failed to be delivered to the destination. Undelivered packet are retransmitted a number of times before an error occurs.

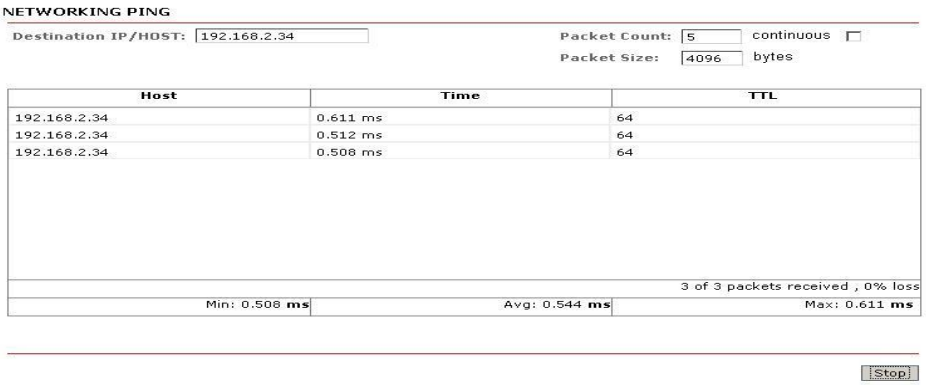
Missed beacons value represents the number beacons (management packets sent at regular intervals by the Access Point) which were missed by the client. This can indicate that the wireless client is out of range.

Other errors value represents the total number of transmitted and received packets that were lost or discarded for other reasons.

More Status

In More Status option contains some useful tools and additional status pages.

Ping Utility – a ping tool to test the connectivity between devices.



ARP Table display a list of MAC addresses of the connected devices

ARP TABLE

IP address	HW type	Flags	HW address	Mask	Device
192.168.168.213	0x1	0x2	00:80:48:15:7D:F1	*	br0
192.168.168.204	0x1	0x2	00:30:CE:06:35:10	*	br0

Bridge Table display a list the devices connect to the bridge interface

BRIDGE TABLE

Port No	Mac Address	Is Local	Agein Timer
1	00:30:ce:06:35:10	no	0.19
1	00:30:ce:06:6f:10	no	1.40
2	00:80:48:15:7d:f1	no	0.47
3	00:80:48:65:0b:e7	no	0.61
1	00:80:48:65:ad:bf	yes	0.00
2	00:80:48:65:ad:c0	yes	0.00
2	00:80:48:66:9f:a4	no	0.56
3	06:80:48:65:ad:c0	yes	0.00
3	06:80:48:65:ad:c0	yes	0.00
3	06:80:48:65:ad:c0	yes	0.00

DHCP Active Lease Table display a list of IPs addresses leased to all computers.

DHCP ACTIVE LEASES

HOST NAME	IP ADDRESS	HARDWARE MAC	LEASE EXPIRED TIME
STATION-4	192.168.88.214	00-80-48-15-5D-E1	FRI DEC 31 17:03:32 1999

Close

VLAN Tab

This setup lets the user create virtual local network connection through the device Ethernet only and over wireless connections.
By default **VLAN** mode is disabled and checked on **No VLAN**

VLAN Switch

To setup VLAN network check on **VLAN Switch**

To add a Tag VLAN ID for Ethernet port, type in the ID number select **Tag** and click **Add**
To add a Tag VLAN ID for MAIN wireless SSID, type in the ID number select **Tag** and click **Add**
To add a Tag VLAN ID for VAP1 wireless SSID, type in the ID number select **Tag** and click **Add**
To add a Tag VLAN ID for VAP2 wireless SSID, type in the ID number select **Tag** and click **Add**
To add a Tag VLAN ID for VAP3 wireless SSID, type in the ID number select **Tag** and click **Add**

***** Warning:** Adding a Tag VLAN ID to device interface port can cause lost of connection to device web manager if the PC ethernet port or wireless connection do not have a Tag VLAN ID or do not have the same Tag VLAN ID setup in device. If this happened, use the device Reset button to clear the config and reconfigure. Refer Reset button operations section.

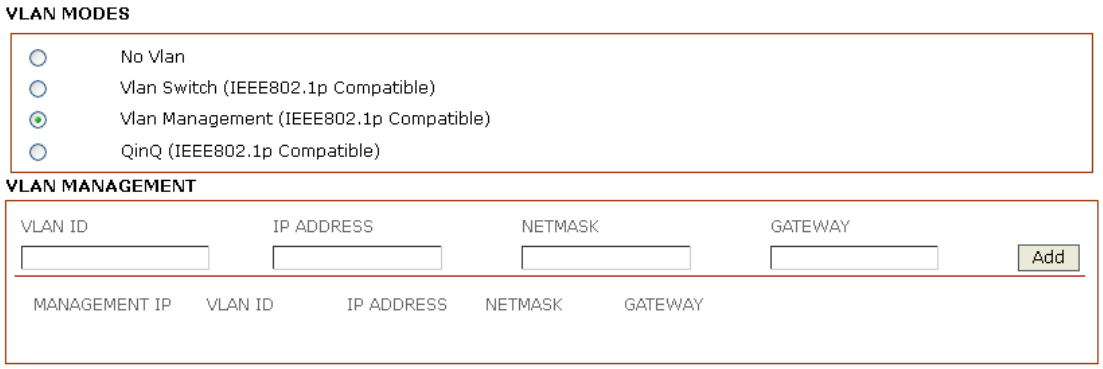
Similarly, to add an untagged VLAN ID, enter the ID number and select **Untag** and click **Add**

Refer to **Appendix V** for VLAN setup examples.

VLAN Management

VLAN management lets the user control and limit only clients connection of same tag VLAN ID group is open AP device web page.

*** Note:-**
VLAN Management works only in tag VLAN pass-through mode. i.e. VLAN Switch is disabled.
When VLAN Switch is enabled or configured, VLAN Management function stops operation.



Example:
Assuming there are 2 VLAN ID groups, 2001 and 2002 setup in AP device.
One entry in VLAN Management has VLAN ID 2001 with masquerade IP address 192.168.168.20
Another entry in VLAN Management has VLAN ID 2002 with masquerade IP address 192.168.168.10
You can only select one of the 2 entries to be the active VLAN ID and IP address.
If VLAN ID 2001 group is selected, then only computers in that VLAN ID group can open the AP device web page using the IP address.
To change to other ID group say, VLAN ID 2002, mark the radio button under Management IP, then click Apply and Saved.

If there is no entry in VLAN Management, there is no restriction. All computers can open the AP device web page by the default IP address setup in Basic Network page.

Appendix I - Network

This section provides more detailed explanation on the network operation modes in general.
The Network Page allows the administrator to Setup Bridge. The IP configuration as described below is required for device management purposes. IP addresses can either be retrieved from a DHCP server or configured manually. Use the Network menu to configure the IP settings.

Network Mode Selections

Network Mode: Specify the operating network mode for the device.
The mode depends on the network topology requirements:

Bridge operating mode is selected by default as it is widely used by the subscriber stations, while connecting to Access Point or using WDS. In this mode the device will act as a transparent bridge and will operate in Layer 2. There will be no network segmentation while broadcast domain will be the same. Bridge mode will not block any broadcast or multicast traffic. Additional Firewall settings can be configured for Layer 2 packet filtering and access control in Bridge mode.

Bridge Mode

Bridge Mode Network Settings

In bridge mode the device forwards all the network management and data packets from one network interface to the other without any intelligent routing. For simple applications this provides efficient and fully transparent network solution. WLAN (wireless) and LAN (Ethernet) interfaces belong to the same network segment which has the same IP address space. WLAN and LAN interfaces form the virtual bridge interface while acting as the bridge ports. The bridge has assigned IP settings for management purposes:

Bridge IP Address:
The device can be set for static IP or can be set to obtain an IP address from the DHCP Server it is connected to. One of the IP assignment modes must be selected:

DHCP: choose this option to assign the dynamic IP address, Gateway and DNS address by the local DHCP server.
STATIC: choose this option to assign the static IP settings for the bridge interface.
IP Address: enter the IP address of the device while Static Bridge IP Address mode is selected. This IP will be used for the device management purposes.
IP Address and Netmask settings should consist with the address space of the network segment where device resides. If the device IP settings and administrator PC (which is connected to the device in wired or wireless way) IP settings will use different address space, the device will become unreachable.

Netmask: This is a value which when expanded into binary provides a mapping to define which portions of IP address groups can be classified as host devices and network devices. Netmask defines the address space of the network segment where device resides. 255.255.255.0 (or /24) Netmask is commonly used among many C Class IP networks.

Gateway IP: Typically, this is the IP address of the host router which provides the point of connection to the internet. This can be a DSL modem, Cable modem, or a WISP gateway router. Device will direct the packets of data to the gateway if the destination host is not within the local network. Gateway IP address should be from same address space (on same network segment) as the device.

Primary/Secondary DNS IP:
The Domain Name System (DNS) is an internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses of where the device looks for the translation source.

Primary DNS server IP address should be specified for the device management purposes. Secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

Appendix III- Advanced Settings

This section provides more detail explanation on advanced setting for routing and wireless settings.

The Advanced options page allows the user to manage advanced settings that influence on the device performance and behavior. The advanced wireless settings are dedicated for more technically advanced users who have a sufficient knowledge about wireless LAN technology.

Advanced Wireless Setting

The 802.11a/g data rates include 6, 9, 12, 18, 24, 36, 48, 54Mbps.

The 802.11n data rates are the MCS (Modulation Coding Scheme) rates.

MCS0 to MCS7 are 802.11n rates, which uses only 1 Tx/Rx stream.

MCS8 to MCS15 are 802.11n rates, which uses 2 Tx/Rx streams.

The Rate Algorithm has a critical impact on performance in outdoor links as generally lower data rates are more immune to noise while higher rates are less immune, but are capable of higher throughput.

Noise Immunity option increases the robustness of the device to operate in the presence of noise disturbance which is usually generated by external 802.11 traffic sources, channel hopping signals and other interferes.

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes, or word “off”. The default value is 2347 which means that RTS is disabled.

RTS/CTS (Request to Send / Clear to Send) is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately. System uses Request to Send/Clear to send frames for the handshake which provide collision reduction for access point with hidden stations. The stations are sending a RTS frame first while data is send only after handshake with an AP is completed. Stations respond with the CTS frame to the RTS which provides clear media for the requesting station to send the data. CTS collision control management has time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.

Fragmentation Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or word “off”. Setting the Fragmentation Threshold too low may result in poor network performance.

The use of fragmentation can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However lower values of the Fragmentation Threshold will result lower throughput as well. Minor or no modifications of the Fragmentation Threshold value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

Acknowledgement Timeout

Device has an auto-acknowledgement timeout algorithm which dynamically optimizes the frame acknowledgement timeout value without user intervention. This is a critical feature required for stabilizing long-distance outdoor links. The user also has the ability to enter the value manually.

Distance: specify the distance value in miles (or kilometers) using slider or enter the value manually. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance.

ACK Timeout: specify the ACK Timeout. Every time the station receives the data frame it sends an ACK frame to the AP (if transmission errors are absent). If the station receives no ACK frame from the AP within set timeout it re-sends the frame. The performance drops because of the too many data frames are re-send, thus if the timeout is set too short or too long, it will result poor connection and throughput performance.
Changing the ACK Timeout''== value will change the Distance to the appropriate distance value for the ACK Timeout.

Auto: Adjust control and enable the ACK Timeout Self-Configuration feature. If enabled, ACK Timeout value will be derived dynamically using an algorithm similar to the Conservative Rate Algorithm described above. It is not recommended to use Auto Adjust option for long range links if the signal level is low or the high level of interference is present.
If two or more stations are located at the considerably different distance from the Access Point, the highest ACK Timeout for the farthest station should be set at the AP side. It is not recommended to use Auto Adjust option for Point-to-Multipoint connections as it will not warrant highest network performance in all the use cases.

Signal Strength LED Settings

LED Thresholds Configuration

The LED's for signal strength on the device can be made to light on when received signal levels reach the values defined in the following fields. This allows a technician to easily deploy a CPE without logging into the unit (i.e. for antenna alignment operation).

Signal LED Thresholds specify the marginal value of Signal Strength (dBm) which will switch on LEDs indicating signal strength:

LED 1 (Red) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 2 (Yellow) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 3 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 4 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.

Configuration example: if the Signal Strength fluctuates around RSSI 15-30, the LED Thresholds can be adjusted to the RSSI values 15, 20, 25, 30.

Appendix IV- Services

Ping WatchDog

The ping watchdog sets the device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the device will automatically reboot. This option creates a kind of "fail-proof" mechanism.
Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. If the defined number of replies is not received, the tool reboots the device.

Enable Ping Watchdog: control will enable Ping Watchdog Tool.
IP Address To Ping: enter the target host IP address to monitor.
Ping Interval: specify time interval (in seconds) between to send the ICMP “echo requests”.
Startup Delay: specify initial time delay (in seconds) from device startup or reboot to start sending first ICMP “echo requests”. Minimum value is 60 seconds.
Failure Count To Reboot: specify the number of ICMP “echo response” replies. If the specified number of ICMP “echo response” packets is not received continuously, the Ping Watchdog Tool will reboot the device.

SNMP Agent

Simple Network Monitor Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. Device contains an SNMP agent which allows it to communicate to SNMP manage applications for network provisioning.
SNMP Agent provides an interface for device monitoring using the Simple Network Management Protocol (an application layer protocol that facilitates the exchange of management information between network devices). SNMP Agent allows network administrators to monitor network performance, find and solve network problems. For the purpose of equipment identification, it is always a good idea to configure SNMP agents with contact and location information:

Enable SNMP Agent: control will enable SNMP Agent.
SNMP Community: specify SNMP community string. It is required to authenticate access to MIB objects and functions as embedded password. The device supports a Read-only community string that gives read access to authorized management stations to all the objects in the MIB except the community strings, but does not allow write access for device that supports SNMP v1.
Contact: specify the identity or contact in case an emergency situation arise.
Location: specify the physical location of the device.

NTP Client, Web, Telnet, SSH Server

NTP Client: The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It can be used to set the device system time. System Time is reported next to the every System Log entry while registering system events if Log option is enabled.
Web Server: the following the device Web Server parameters can be set there:
Use Secure Connection (HTTPS): If checked Web server will use secure HTTPS mode. HTTP mode is selected by default.
Secure Server Port: Web Server TCP/IP port setting while using HTTPS mode.
Server Port: Web Server TCP/IP port setting while using HTTP mode.

Telnet Server: the following the device Telnet Server parameters can be set there:
Enable Telnet Server: Enables Telnet access to the device.
Server Port: Telnet service TCP/IP port setting.

SSH Server: the following the device SSH Server parameters can be set there:
Enable SSH Server: Enables SSH access to the device.
Server Port: SSH service TCP/IP port setting.

System Log

Enable Log: option enables the registration routine of the system log messages. Enable Remote Log enables the syslog remote sending function while System log messages are sent to a remote server specified by the Remote Log IP Address and Remote Log Port.

Remote Log IP Address is the host IP address where syslog messages should be sent. Remote host should be configured properly to receive syslog protocol messages.
Remote Log Port is the TCP/IP port of the host syslog messages should be sent. "514" is the default port for the commonly used system message logging utilities
.
Every logged message contains at least a *System Time* and a Host Name. Usually a particular service name which generates the system event is specifies also within the message. Messages from different services have different context and different level of the details. Usually *error*, *warning* or *informational* system services messages are reported. The more detailed system messages are reported, the greater volume of log messages will be generated.

uConfig Utility

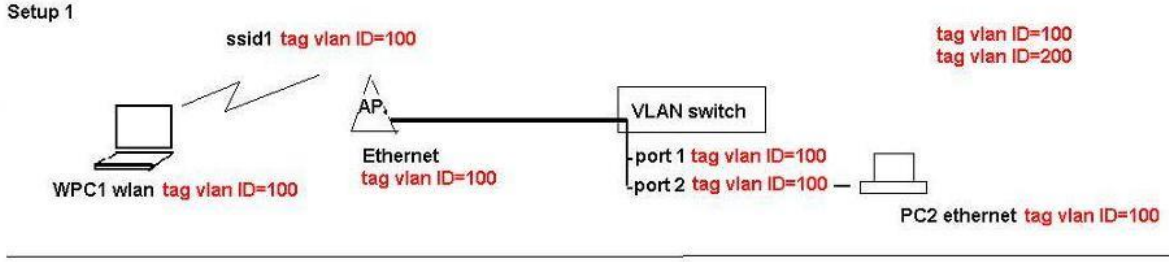
The exclusive uConfig utility allows users to access the user-friendly Web configuration interface of the access point without having to change the TCP/IP setup of the workstation.

Appendix V- VLAN Setup examples

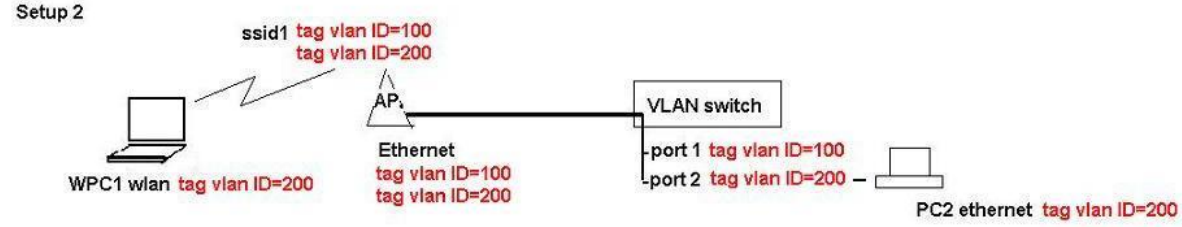
A) Tagged Wireless VLAN to Tagged Ethernet VLAN Setup

Tag vlan connection Setup

Setup 1



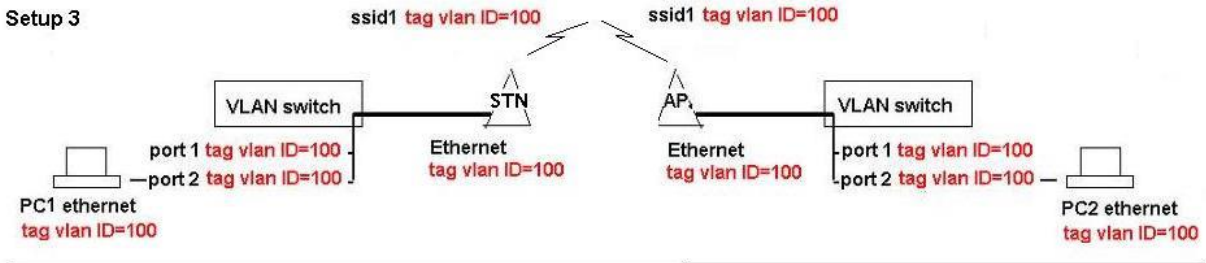
Setup 2



Hints:-

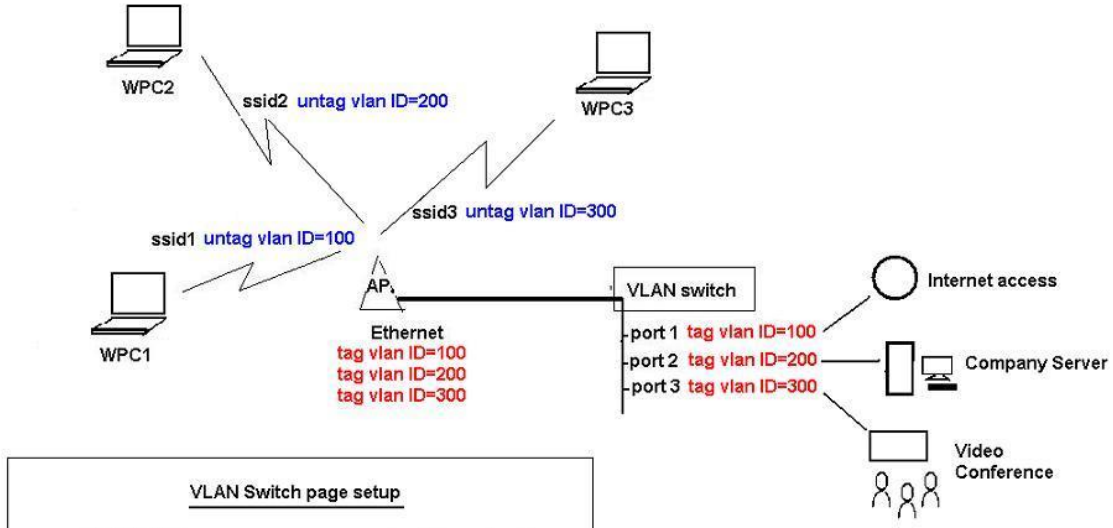
For each vlan id group to send between AP and wireless clients,
AP wlan and ethernet interface must add that vlan group.
AP ethernet port connecting to the switch must set to the default vlan id same as switch port its connecting.

Setup 3



B) Untagged Wireless VLAN to Tagged Ethernet VLAN setup

Multi-SSID with untag vlan connections to secured wired tag vlan network connections



VLAN Switch page setup

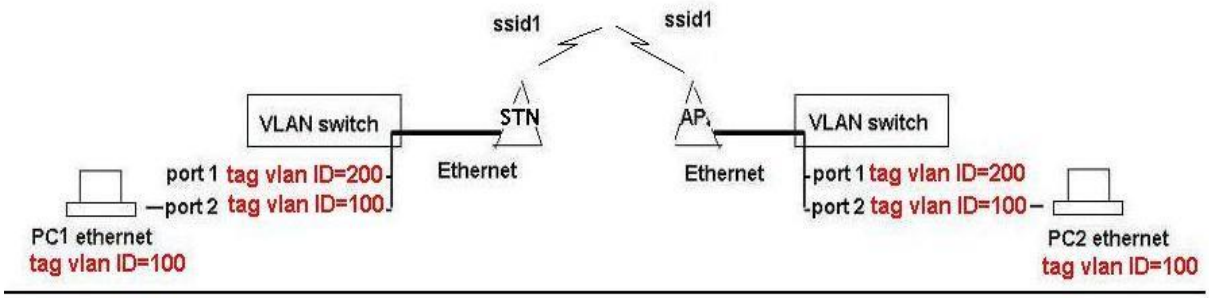
	for wireless	for Ethernet port
MAIN	add untag vlan ID=100	add tag vlan ID=100
VAP1	add untag vlan ID=200	add tag vlan ID=200
VAP2	add untag vlan ID=300	add tag vlan ID=300
VAP3	add untag vlan ID=400	add tag vlan ID=400

C) Tagged VLAN Pass-Through

AP and Station link No VLAN Setup Required

Tagged VLAN pass-through. AP and Station link no VLAN Setup Required

*** - AP and Station devices no VLAN setting required**



Technical Specification

The APX-110N5 and APX-120N5 – Outdoor IP67 Wireless Bridge technical specifications are shown below.

Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX Fast Ethernet IEEE 802.11i 256-bit Pre-shared Key Supported IEEE802.3x Flow Control and Back Pressure IEEE802.3af Power over Ethernet
Protocol	CSMA/CD
Data Rate	Maximum data rate 300Mbps
MAC Address	2K Table size
RJ45 Port	1 PoE PD (Power Device) 10/100BaseT(X) auto negotiation speed and auto MDI/MDI-X connection
PoE Pin Assignment	RJ-45 port support IEEE 802.3af Positive (VCC+): RJ-45 pin 1, 2. Negative (VCC-): RJ-45 pin 3, 6. Data (1,2,3,6)
LED	**Power**: On: Power is received; Off: No PoE detected **Ethernet**: On: A link to PC or switch is present Off: No link is detected **Signal:** On: Sufficient signal strength to establish the connection Off: No wireless connection has been made **Diag**: On: When a wireless connection has been made Off: On start up or when a wireless connection has not been established
Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5, 5e cable EIA/TIA-568 100-ohm (100m) 100Base-TX: 2-pair UTP/STP Cat. 5/5e, 6 cable EIA/TIA-568 100-ohm (100m)
Power Input	IEEE 802.3af PoE
Max Power Consumption	7.5 watts
Installation	Pole Mounting
Operating Temp.	Standard Operating Temperature: -20^{o}C to 70^{o}C

Operating Humidity	5% to 95% (Non-Condensing)
Storage Temperature	-40°C to 85°C
Case Dimension	IP-67, 257mm (W) x 86mm (D) x 257mm (H)
EMI	This device complies with part 15 of the FCC Rules